Revista Integración
Escuela de Matemáticas
Universidad Industrial de Santander
Vol. 24, No. 1, 2006, pág. 31–50

Criptografia usando curvas hiperelípticas

Alonso Sepúlveda Castellanos*

Resumo. Neste trabalho apresentamos propriedades das curvas hiperelípticas e seus Jacobianos, visando a implementação de criptossistemas de chave pública. Também mostramos o algoritmo de Cantor para somar pontos na variedade Jacobiana, importante para efetividade dos criptossistemas, e um algoritmo para atacar o problema do logaritmo discreto sobre estes grupos. A intratabilidade deste problema é essencial para a segurança do criptossistema.

Abstract. In this work we present properties of the hiperelípticas curves and its Jacobianos, aiming at the implementation of criptossystems of public key. Also we show the algorithm of Singer to add points in the Jacobiana variety, important for effectiveness of criptossystems, and an algorithm to attack the problem of the discrete logarithms on these groups. The not tractably of this problem is essential for the security of criptossystems.

1. Introdução

Em 1989 Koblitz [4] introduziu pela primeira vez os criptossistemas hiperelípticos, os quais baseiam sua segurança na resolução do problema do logaritmo discreto sobre o Jacobiano da curva. Introduzimos a teoria básica de curvas hiperelípticas e seus Jacobianos com o fim de propor grupos que sirvam para implementar criptossistemas de chave pública. Fixamos K um corpo perfeito de característica $p \geq 0$, $\bar{K}$ seu fecho algébrico e g um inteiro positivo.

Palavras chaves: Criptografia, Curvas Hiperelípticas, Logaritmo Discreto.
MSC2000: Primaria: 11T71, 11G05. Secundaria: 11G16, 94A60.

* Bolsista do Cnpq, Instituto de Matemática, Estatistica e Computação Cientifica IMECC, Unicamp-Brasil, *e-mail*: alonsosc@ime.unicamp.br.

1.1. Generalidades

As curvas hiperelípticas são uma classe especial de curvas algébricas e podem ser vistas como uma generalização das curvas elípticas [1].

Definição 1.1. Uma curva hiperelíptica **H** sobre K são os zeros no plano projetivo $\mathbb{P}^2(\bar{K})$ de uma equação da forma

$$Y^2Z^{2g-1} + h(X/Z)YZ^{2g} = f(X/Z)Z^{2g+1}\,, \tag{1}$$

onde

(1) $f \in K[X]$, mónico e de grau $2g+1$;

(2) $h \in K[X]$, $h = 0$ ou de grau no máximo g;

(3) A curva **H** é não singular em todo ponto $P = (x : y : 1)$.

O número g é um invariante da curva chamado o *gênero*, (veja [3, p. 196]). A condição (3) na definição acima é equivalente a que o sistema

$$\begin{aligned} Y^2 + h(X)Y - f(X) &= 0,\\ 2Y + h(X) &= 0,\\ h(X)'Y - f'(X) &= 0 \end{aligned}$$

não tenha solução em $\bar{K} \times \bar{K}$. Da equação (1) temos que a curva **H** intercepta a reta $Z = 0$ no ponto

$$\mathcal{O} = (0 : 1 : 0)\,,$$

e assim podemos considerar a **H** como sendo a união deste ponto com os zeros $(X, Y) \in \bar{K} \times \bar{K}$ do polinômio

$$F = F(X, Y) := Y^2 + h(X)Y - f(X)\,. \tag{2}$$

Se a característica p é maior que dois, então o polinômio da equação (2) pode ser considerado como $F = Y^2 - f(X)$ fazendo a mudança de variáveis: $Y \mapsto Y - h(X)/2$, com $f(X)$ um polinômio mônico de grau $2g+1$.

Seja L um corpo tal que $K \subseteq L \subseteq \bar{K}$. O conjunto $\mathbf{H}(L)$ de pontos racionais de **H** sobre L está formado pelo ponto $\mathcal{O}$ e os zeros $(x, y) \in L \times L$

do polinômio F em (2). Para $K = \mathbb{F}_q$ e $L = \mathbb{F}_{q^n}$, denotamos por n_L o número de pontos racionais de $\mathbf{H}$ sobre L; então

$$n_L = q^n + 1 - \sum_{i=1}^{g} (\alpha_i + \bar{\alpha}_i)\,, \tag{3}$$

onde os α_i, $i = 1, \ldots, g$, são inteiros algébricos tal que $|\alpha_i| = q^{n/2}$. Temos que

$$\alpha_i = \beta_i^n\,, \qquad \text{para } i = 1, \ldots, g, \tag{4}$$

onde os β_i e seus conjugados são raízes de um polinômio com coeficientes em $\mathbb{Z}[t]$ da forma

$$h(t) = t^{2g} + a_1 t^{2g-1} + \ldots + a_g t^g + q a_{g-1} t^{g-1} + q^2 a_{g-2} t^{g-2} + \ldots + q^{g-1} a_1 t + q^g\,. \tag{5}$$

De (3) obtemos a chamada cota de Hasse-Weil para $\mathbf{H}(L)$, a saber,

$$|n_L - (q^n + 1)| \leq 2\sqrt{q^n} g\,.$$

Agora seja $S_i := \#\mathbf{H}(\mathbb{F}_{q^i}) - (q^i + 1)$. De (3) e (4) aplicados com $n = i$, temos

$$S_i = -\sum_{j=1}^{g} (\beta_i^n + \bar{\beta}_i^n)\,, \qquad \text{para } i \geq 1\,.$$

Assim por exemplo, da Equação (5), $a_1 = S_1$, $2a_2 = S_2 + S_1 a_1$, e em geral temos as seguintes fórmulas de recorrência utilizando as fórmulas de Newton (ver [6, Cor. V.1.17]):

$$i a_i = S_i + \sum_{j=1}^{i-1} S_{i-j} a_j\,.$$

Vemos então que o polinômio $h(t)$ em (5) se determina completamente se conhecemos S_i para $i = 1, \ldots, g$. Em particular, com esta informação podemos calcular $\#\mathbf{H}(\mathbb{F}_{q^i})$ para $i \geq g + 1$.

Sobre $\mathbf{H}$ está definida uma *involução* $\sigma : \mathbf{H} \to \mathbf{H}$ definida por $(x, y) \mapsto (x, -y - h(x))$ e $\sigma(\mathcal{O}) = \mathcal{O}$. Este automorfismo será essencial para determinar os divisores reduzidos sobre a o Jacobiano da curva.

Um *divisor* D sobre $\mathbf{H}$ é uma soma formal de pontos de $\mathbf{H}$, $D = \sum_P v_P(D) P$, onde cada $v_P(D)$ é um inteiro e diferente de zero somente para um número finito de pontos. O conjunto $\sup(D)$ dos pontos P onde $v_P(D) \neq 0$ é chamado de *suporte* de D. O conjunto de divisores de $\mathbf{H}$ será denotado por $\mathrm{Div}(\mathbf{H})$.

O *grau* de um divisor D está definido por $\deg(D) := \sum_P v_P(D)$. Para um corpo L tal que $K \subseteq L \subseteq \bar{K}$, dizemos que D *está definido sobre* L, se para todo automorfismo τ de $\mathbf{H}$ definido sobre L temos que $D^\tau = D$. Para dois divisores $D_1 = \sum_P v_P(D_1)P$, $D_2 = \sum_P v_P(D_2)P \in \mathrm{Div}_L(\mathbf{H})$, definimos

$$\mathrm{mdc}(D_1, D_2) := \sum_{P \neq \mathcal{O}} \min\{v_P(D_1), v_P(D_2)\}P - m\mathcal{O}\,,$$

com $\deg(\mathrm{mdc}(D_1, D_2)) = 0$. Definamos

$$\mathrm{Div}_L^0(\mathbf{H}) := \mathrm{Div}_L(\mathbf{H}) \cap \mathrm{Kernel}(\deg);$$

este conjunto é um subgrupo de $\mathrm{Div}_L(\mathbf{H})$.

1.2. Corpo de funções racionais

Os elementos do anel $L[\mathbf{H}] := L[X, Y]/(F)$, onde (F) é o ideal de $L[X, Y]$ gerado por F, podem ser considerados *funções polinomiais* $g : \mathbf{H} \to \mathbb{P}^1(\bar{K})$ com $g(P) = \infty$ se e somente se $P = \mathcal{O}$. Sendo F absolutamente irredutível, $L[\mathbf{H}]$ é um domínio de integridade, e portanto está definido seu corpo quociente $L(\mathbf{H})$; este é chamado o Corpo de Funções Racionais de $\mathbf{H}$ sobre L. Para $R \in L[X, Y]$, denotemos por $\bar{R}$ a sua classe em $L[\mathbf{H}]$. Podemos identificar cada constante $a \in L$ con $\bar{a}$ e X com $\bar{X}$. Seja $y := \bar{Y}$. Então tomando classes, temos que $F(X, y) = 0$, isto é,

$$y^2 + h(X)y - f(X) = 0\,.$$

Desta forma, cada elemento de $L[\mathbf{H}]$ pode ser reduzido de maneira única para polinômios da forma

$$A(X) + B(X)y\,.$$

Observe que isto significa que $L[\mathbf{H}]$ é um módulo livre de posto dois sobre $L[X]$. Finalmente, temos que $L(\mathbf{H}) = L(X, y)$, pois $[L(\mathbf{H}) : L(X)] = 2$ e $[L(\mathbf{H}) : L(y)] = 2g + 1$.

Seja $L = \bar{K}$. Seja $r \in \bar{K}(\mathbf{H})$, $P \in \mathbf{H}$, $P \neq \mathcal{O}$. Dizemos que r está definida em P ou que r é *regular* em P, se existem funções polinomiais R, S tais que $r = R/S$ e $S(P) \neq 0$; neste caso $r(P) := R(P)/S(P)$.

No caso de que r não possa ser definido em P, este ponto é dito um *pólo* de r, e definimos $r(P) := \infty$. Se r está definido em P e $r(P) = 0$, P é chamado de zero de r. Observamos que $r \neq 0$ tem um número finito de polos e zeros. Com efeito, os zeros $P = (a_P, b_P)$ de r são os zeros de uma

função polinomial da forma $A(X)+B(X)y$, onde $A, B \in \bar{K}[X]$. Podemos supor $\mathrm{mdc}(A(X), B(X)) = 1$, logo

$$(A(X) + B(X)y)(A(X) - B(X)(y + h(X)))$$

é uma função polinomial em X e portanto o número de coordenadas a_P para P é finito. Como $A(a_P) + B(a_P)b_P = 0$ e $B(a_P) \neq 0$ (do contrário $(X - a_P)$ será um divisor de $A(X)$ e $B(X)$), então $b = -A(a_P)/B(a_P)$. O mesmo raciocínio serve para os pólos.

1.3. Divisores principais

A cada função racional não nula r associamos um divisor de grau zero sobre $\mathbf{H}$, chamado de divisor principal:

$$\mathrm{div}(r) := \sum_{P \in \mathbf{H}} v_P(r)P\,,$$

onde $P \in \sup(\mathrm{div}(r))$ se e somente se P é um zero ou P é um polo de r. Para $P \in \mathbf{H}$ e $r = 0$, $v_P(0) := +\infty$. Em $\bar{K}(\mathbf{H}) \setminus \{0\}$ temos que v_P satisfaz as seguintes propriedades:

(1) $v_P(rr_1) = v_P(r) + v_P(r_1)$;

(2) $v_P(r + r_1) \geq \min\{v_P(r), v_P(r_1)\}$ (e temos a igualdade se $v_P(r) \neq v_P(r_1)$).

Neste caso v_P é chamada de *valoração* ou de *ordem* em P. Para $r = R/S \in \bar{K}(\mathbf{H})$, $r \neq 0$, $v_P(r)$ será por definição $v_P(R) - v_P(S)$. Denotamos o conjunto destes divisores por $P_{\bar{K}}(\mathbf{H})$ e dizemos que dois divisores D_1 e D_2 sobre $\mathbf{H}$ são linearmente equivalentes, escrevemos $D_1 \sim D_2$, se $D_1 - D_2$ é um divisor principal.

1.4. Divisores semi-reduzidos

Um divisor de grau zero $D = \sum_{P \neq \mathcal{O}} v_P(D)P - m\mathcal{O}$, onde $m \geq 0$, $v_P(D) \geq 0$ para todo P, é chamado semi-reduzido se:

- Para P tal que $\sigma(P) \neq P$, se $P \in \sup(D)$ então $\sigma(P) \notin \sup(D)$;
- Se $\sigma(P) = P$, com$P \neq \mathcal{O}$, $v_P(D) = 1$.

Lema 1.2. Todo divisor de grau zero é linearmente equivalente a um divisor semi-reduzido.

Demonstração. Temos

$$D = \sum_{P \in \mathbf{H}} v_P(D)P = \sum_{P, P \neq \sigma(P)} v_P(D)P + \sum_{P \neq \mathcal{O}, \sigma(P)=P} v_P(D)P - m\mathcal{O}\,.$$

Seja $P \neq \sigma(P)$ e definamos $m_P := \min\{v_P(D), v_{\sigma(P)}(D)\}$. Logo

$$v_P(D)P + v_{\sigma(P)}(D)\sigma(P) \sim 2m_P\mathcal{O} + (\max\{v_P(D), v_{\sigma(P)}(D)\} - m_P)R\,,$$

onde R é P ou $\sigma(P)$.
Se $P = \sigma(P)$, e $n_P := v_p(D)$ é um inteiro par, temos $n_P P \sim n_P\mathcal{O}$; caso contrário se $n_P = 2n + 1$, $n_P P \sim 2n\mathcal{O} + P$. ☑

1.5. Divisores reduzidos

Fixemos D um divisor semi-reduzido,

$$D = \sum_{P=\sigma(P), P\neq\mathcal{O}} P + \sum_{P\neq\sigma(P)} v_P(D)P - m\mathcal{O}\,.$$

D è chamado *reduzido* se $\sum_{P\neq\mathcal{O}} v_P(D) = m \leq g$, onde g é o gênero de $\mathbf{H}$.

Teorema 1.3. Existe um único divisor reduzido D_1 tal que $D \sim D_1$.

A seguir mostraremos um lema que será de grande utilidade na demonstração do teorema acima. Assim, seja D_1 um divisor de grau zero, pelo lema (1.2) podemos supor que $D_1 \sim D$. Para $P \in \sup(D) \setminus \{\mathcal{O}\}$, $P = (a_P, b_P)$, definamos

$$A = A(X) := \prod_P (X - a_P)^{v_P(D)} \in \bar{K}[X]\,.$$

Lema 1.4. Existe um único polinômio $B = B(X) \in \bar{K}[X]$ tal que:

(1) $\deg(B) < \deg(A)$;

(2) Para $P \in \sup(D) \setminus \{\mathcal{O}\}$, $B(a_P) = b_P$;

(3) $B^2 + Bh(X) - f(X) \equiv 0 \pmod{A}$.

Além disso, $D = \mathrm{div}(A, B) := \mathrm{mdc}(\mathrm{div}(A), \mathrm{div}(B - y))$. Para $r \in \bar{K}(\mathbf{H})$, observamos que a notação $r \equiv 0 \pmod{A}$ significa que $r = As$ onde $v_P(s) \geq 0$.

Demonstração. Primeiro mostramos uma versão local do lema. ☑

Afirmação: Para $P \in \sup(D)$, $P \neq \mathcal{O}$, existe um único polinômio $R = R_P(X)$ tal que

(i) $\deg(R) < v_P(D)$, (ii) $R(a_P) = b_P$,

(iii) $R^2 + Rh(X) - f(X) \equiv 0 \pmod{(X - a_P)^{v_P(D)}}$.

Caso $P \neq \sigma(P)$**.** Como $v_P((y - b_P)/(x - a_P)) \geq 0$, $y = b_P + (X - a_P)A$, com único $A \in \bar{K}(\mathbf{H})$ tal que $v_P(A) \geq 0$. Repetindo este processo por substituições do tipo $A = (A - A(P)) + A(P)$, obtemos uma única representação para y do tipo

$$y = b_P + c_1(X - a_P) + \ldots + c_{v_P(D)-1}(X - a_P)^{v_P(D)-1} + (X - a_P)^{v_P(D)} R_1 \,,$$

onde $v_P(R_1) \geq 0$. Logo definimos

$$R = R_P(X) := b_P + c_1(X - a_P) + \ldots + c_{v_P(D)-1}(X - a_P)^{v_P(D)-1} \,.$$

Este polinômio claramente satisfaz (i), (ii) e a propriedade (iii) segue do fato que $y \equiv R \pmod{(X - a_P)^{v_P(D)}}$ (observe que $v((R - y)/(x - a_P)^{v_P(D)} \geq 0$ pois $R - y = (x - a_P)^{v_P(D)})R_1$).

Caso $P = \sigma(P)$**.** Aqui $v_P(D) = 1$, e temos que $R = R_P := b_P$. Para demonstrar a forma global do teorema, aplicamos o Teorema Chinês dos Restos em A e os R_P, e daí obtemos que existe um único polinômio $B = B(X)$ tal que $\deg(B) < \deg(A)$ e $B(X) \equiv R_P \pmod{(X - a_P)^{v_P(D)}}$. Este B claramente satisfaz (1) e (2), (3) é devido ao fato de que os fatores de A são co-primos entre si. A unicidade segue-se da prova. Finalmente mostramos que D é o mdc dos divisores $\mathrm{div}(A)$ e $\mathrm{div}(B - y)$.

Seja $P = (a, b)$ tal que $P = \sigma(P)$; temos que $v_P(B - y) \geq 1$ por (2) e que $v_P(A) = 2$. Para mostrar que de fato $v_P(B - y) = 1$, consideremos a função

$$N = N(X) := B^2 + Bh(X) - f(X) = (B - y)(B + y + h);$$

logo (2) implica $v_P(N) \geq 1$. Afirmamos que $v_P(N) = 1$; para isto bastará mostrar que $N'(a) \neq 0$. Temos $N'(X) = 2BB' + B'h(X) + Bh(X)' - f(X)'$. Logo, avaliando em P, usando (2) e o fato que $b = -b - h(a)$, obtemos $N'(a) = bh'(a) - f'(a) \neq 0$, pois $\mathbf{H}$ é não singular em P. Obtemos assim que $v_P(D) = 1$.

Seja P tal que $P \neq \sigma(P)$. De (3), $(R-y)(R+y+h(X)) = R^2+Rh(X)-f(X) = Ar$ onde $v_P(r) \geq 0$. Logo $v_P(B-y) = v_P(A)+v_P(r)$, pois P não é ponto fixo. Portanto, o $\mathrm{mdc}(A, B-y) = \sum_{P\neq\mathcal{O}} v_P(D)P - m\mathcal{O} = D$. ☑

Observação 1.5. Sejam A e B dois polinômios satisfazendo as condições (1) e (3) do lema anterior. Então o divisor $D := \mathrm{mdc}(\mathrm{div}(A), \mathrm{div}(B-y))$ é semi-reduzido.

Demonstração. Seja $P = (a_P, b_P) \in \sup(\mathrm{div}(A))$. Para $P \neq \sigma(P)$ e de (3) temos que $v_P(B-y) = v_P(A)+v_P(s)$ onde $v_P(s) \geq 0$, logo $v_P(B-y) \geq v_P(A)$ e $v_{\sigma(P)}(B-y) = 0$. Para $P = \sigma(P)$ e da condição (3) segue-se $(B-y)(P) = 0$, logo $v_P(B-y) \geq 1$. Afirmamos que $v_P(B-y) = 1$. Dado

$$N(X) = (B-y)(B+y+h) = B^2 + Bh - f,$$

temos que $N(a_P) = 0$ e $N'(a_P) \neq 0$, pois $P \neq \mathcal{O}$ não é ponto singular da curva. ☑

Demonstração do Teorema 1.3. Primeiro mostramos a existência de este tipo de divisores. Podemos supor que $D = D_0 := D_0^0 - m\mathcal{O}$ é um divisor semi-reduzido do Lema 1.2 tal que $\sum_{P\neq\mathcal{O}} v_P(D_0) \geq g+1$, onde g é o gênero de $\mathbf{H}$. Assim, podemos escolher $P_1, \ldots, P_{g+1}$ do suporte de D (não necessariamente diferentes) e considerar o divisor semi-reduzido

$$E = E_0 := P_1 + \ldots + P_{g+1} - (g+1)\mathcal{O}\,.$$

Pelo lema anterior, existem polinômios $A = A_0$ e $B = B_0$ tal que

$$\mathrm{div}(B-y) = P_1 + \ldots + P_{g+1} + Q_1 + \ldots + Q_g - (2g+1)\mathcal{O}.$$

Seja $D = F_0 + P_1 + \ldots + P_{g+1} - m\mathcal{O}$. Logo

$$D - \mathrm{div}(B-y) = F_0 - Q_1 - \ldots - Q_g - (m-2g-1)\mathcal{O} \sim D_1 := D_0^1 - (m-1)\mathcal{O}\,,$$

sendo que D_1 pode ser assumido semi-reduzido. Agora a prova de existência termina por indução sobre m, pois o grau do novo divisor construído, no mínimo diminui em 1.

Para mostrar a unicidade destes divisores, escolhemos D_1, D_2 divisores reduzidos tal que $D \sim D_1$ e $D \sim D_2$. Como $\deg(D_1 - D_2) = 0$, pelo Lema 1.2, $D_1 - D_2 \sim D_3$, onde D_3 é o divisor semi-reduzido obtido da prova do lema. Seja $P \in \mathbf{H}$ tal que $m := v_P(D_1) \neq n := v_P(D_2)$; considerando $D_1 - D_2$ ou $D_2 - D_1$, podemos supor que $m \geq 1$ e que algum dos seguintes casos podem ocorrer:

(1) $n = 0$ e $v_{\sigma(P)}(D_2) = 0$;

(2) $1 \leq n < m$;

(3) $1 \leq v_{\sigma(P)}(D_2) \leq m$.

Logo pela escolha de D_3 temos que $v_P(D_3) \geq 1$ para todos os casos acima. De fato, nos Casos (1) e (2) $v_P(D_3) = (m - n) \geq 1$ e no caso (3) $\sigma(P) \neq P$; da propriedade $P + \sigma(P) \sim 2\mathcal{O}$ e da construção de D_3 segue a afirmação. Agora como $D_3 \sim 0$, existe $r \in \bar{K}(\mathbf{H})$ tal que $D_3 = \mathrm{div}(r)$; pela definição de D_3, o único polo de r é $\mathcal{O}$ e assim $r = A(X) + B(X)y$, onde $A(X), B(X) \in \bar{K}[X]$. Para $i = 1, 2, 3$ escrevamos $D_i = \sum_{P \neq \mathcal{O}} v_{P(i)}(D_i)P - d_i\mathcal{O}$, onde $d_i := \sum_{P \neq \mathcal{O}} v_{P(i)}(D_i)$. Pela definição de divisor reduzido, $d_1 \leq g$ e $d_2 \leq g$, pelo tanto fica claro que $d_3 \leq 2g$.

Mostraremos que $B(X) = 0$. Suponhamos que $B(X) \neq 0$; como $v_{\mathcal{O}}(A(X)) \neq v_{\mathcal{O}}(B(X)y)$, então $v_{\mathcal{O}}(r) = \min\{v_{\mathcal{O}}(A(X)), v_{\mathcal{O}}(B(X)y\}$. Daqui temos que $v_{\mathcal{O}}(B(X)y) < v_{\mathcal{O}}(A(X))$, pois do contrário

$$-2\mathrm{deg}(B(X)) - (2g + 1) \geq v_{\mathcal{O}}(A(X)) = v_{\mathcal{O}}(r) = -d_3 \geq -2g,$$

o qual é falso. Assim temos,

$$v_{\mathcal{O}}(B(X)) - (2g + 1) = v_{\mathcal{O}}(r) = -d_3$$

e daí $d_3 \geq 2g + 1 + 2\mathrm{deg}(B(X))$, o que não verdade; portanto $r = A(X)$ com $\mathrm{deg}(A(X)) \geq 1$. Tome $Q = (a, b) \in \mathbf{H}$ tal que $A(a) = 0$, logo pela definição de $\sigma(Q)$, temos que $Q, \sigma(Q) \in \mathrm{sup}(D_3)$, o qual é contraditório com a definição de D_3. Logo concluímos que $D_1 = D_2$. ☑

2. O Jacobiano de $\mathbf{H}$

O *Jacobiano* $\mathcal{J} = \mathcal{J}_{\mathbf{H}}$ de $\mathbf{H}$ é o grupo quociente

$$\mathrm{Div}^0/P\,,$$

onde $\mathrm{Div}^0 = \mathrm{Div}^0_{\mathbf{H}}$ é o grupo de divisores de grau zero sobre $\mathbf{H}$ e $P = P_{\mathbf{H}}$ é o subgrupo de divisores principais de Div^0.

2.6. Pontos racionais do Jacobiano

Para aplicações criptográficas usando o método Diffie-Hellman ou ElGamal, é de interesse o estudo de subgrupos finitos do Jacobiano da curva

hiperelíptica escolhida. Em nosso caso, consideraremos subgrupos finitos do Jacobiano da curva definida sobre $K = \mathbb{F}_q$. É um fato que $\mathcal{J}$ está também definido sobre K. Seja L uma extensão finita de K e D um divisor definido sobre L. Pelo Teorema 1.3 existe um único divisor reduzido $D_1 = \sum_P v_P(D_1)P$ tal que $D \sim D_1$, e pela denifinição de divisor reduzido temos que $\sum_P v_P(D_1) \leq g$, onde g é o gênero da curva. Assim, existe um número finito de possibilidades para obter divisores reduzidos, logo obtemos um número finito de elementos do Jacobiano. Seja $K := \mathbb{F}_q$, $L = \mathbb{F}_{q^n}$ e $N_L := \#\mathcal{J}_L(\mathbf{H})$. Se sabe que N_L pode-se calcular a partir dos inteiros α_i em (3). De fato temos [6, Theorem. V1.15]

$$N_L = \prod_{i=1}^{g}(1-\alpha_i)(1-\bar{\alpha}_i)\,. \tag{6}$$

Logo, usando que $|\alpha_i| = q^{n/2}$, se obtém:

$$(q^{n/2}-1)^{2g} \leq N_L \leq (q^{n/2}+1)^{2g}\,.$$

Exemplo 2.1. Consideremos a curva $\mathbf{H}$ definida pelo polinômio $F(X,Y) := Y^2 + Y - X^3 - X = 0$, então para $L = \mathbb{F}_q^n$ temos que:

$$N_L := \#\mathcal{J}_L(\mathbf{H}) = \begin{cases} 2^{2n}+2^n+1 & \text{se } n \equiv 1,5 \pmod 6, \\ (2^n+2^{n/2}+1)^2 & \text{se } n \equiv 2,4 \pmod 6, \\ (2^n-1)^2 & \text{se } n \equiv 3 \pmod 6, \\ (2^{n/2}-1)^4 & \text{se } n \equiv 0 \pmod 6. \end{cases}$$

Seja $L = \bar{K}$. Pelo Teorema 1.3, a cada classe $[D] \in \mathcal{J}_{\bar{K}}$ lhe corresponde um único divisor reduzido D_R. De fato o mapa $[D] \mapsto D_R$ define um sistema completo de representantes para os elementos de $\mathcal{J}_{\bar{K}}(\mathbf{H})$.

2.7. Soma de Divisores no Jacobiano

Aqui apresentaremos o algoritmo de Koblitz [4], que é uma generalização dos algoritmos de Cantor [2] para computar eficientemente a soma de divisores reduzidos no $\mathcal{J}_L(\mathbf{H})$, o qual só fez para o caso em que a característica do corpo era diferente de dois e $h(X) = 0$. A seguir descrevemos em forma geral estes algoritmos.

- **Algoritmo 1**. Dados dois divisores $D_1, D_2 \in \mathcal{J}_{\mathbb{F}_q}(\mathbf{H})$ semi-reduzidos, ao aplicar o algoritmo este devolve um divisor D_0 semi-reduzido, equivalente ao divisor $D_1 + D_2$.

- **Algoritmo 2**. Dado um divisor semi-reduzido D_0 de grau ℓ_0, ao aplicar o algoritmo, este devolve um divisor D semi-reduzido tal que $D_0 \sim D$ e $\ell < \ell_0$, onde ℓ é o grau de D. Aplicando sucessivamente este algoritmo achamos um divisor reduzido equivalente a D_0.

A seguir os passos a efetuar para cada algoritmo:

Algoritmo 1. Sejam $D_1 = \mathrm{div}(A_1, B_1)$ e $D_2 = \mathrm{div}(A_2, B_2)$ divisores semi-reduzidos sobre a curva $Y^2 + h(X)Y = f(X)$ definidos sobre K, onde $h, f \in K[X]$ e $A_1, B_1, A_2, B_2 \in K[X]$. A seguir, descrevemos os passos formalmente para aplicar este algoritmo.

(1) Usando o algoritmo de Euclides sobre $K[X]$, achamos $d_1, e_1, e_2 \in K[X]$ tal que

$$d_1 = \mathrm{mdc}(A_1, A_2) \,\mathrm{e}\, d_1 = e_1 A_1 + e_2 A_2.$$

(2) Usando outra vez o algoritmo de Euclides, achamos $d, c_1, c_2 \in K[X]$ tal que

$$d = \mathrm{mdc}(d_1, B_1 + B_2 + h) \,\mathrm{e}\, d = c_1 d_1 + c_2(B_1 + B_2 + h).$$

(3) Sejam $s_1 = c_1 e_1$, $s_2 = c_2 e_2$ e $s_3 = c_2$; então temos que

$$d = s_1 A_1 + s_2 A_2 + s_3(B_1 + B_2 + h). \tag{7}$$

(4) O divisor $D' = \mathrm{div}(A, B)$ é o divisor semi-reduzido equivalente a $D_1 + D_2$, tal que

$$A' = A_1 A_2 / d^2, \tag{8}$$

e

$$B' = \frac{s_1 A_1 B_2 + s_2 A_2 B_1 + s_3(B_1 B_2 + f)}{d} \pmod{A}. \tag{9}$$

A seguir, mostramos que o divisor D' acima, é um divisor semi-reduzido e equivalente a $D_1 + D_2$. A prova está dividida em três partes:

- Mostremos que A' e B' são funções polinomiais. Claramente A' é uma função polinomial, pois d divide A_1 e A_2; então d^2 divide $A_1 A_2$. Usando a equação (7), podemos escrever

$$B' = \frac{s_1 A_1 B_2 + s_2 A_2 B_1 + s_3(B_1 B_2 + f)}{d}$$

como sendo

$$\frac{B_2(d - s_2A_2 - s_3(B_1 + B_2 + h)) + s_2A_2B_1 + s_3(B_1B_2 + f)}{d} = B_2 + \frac{s_2A_2(B_2 - B_1) - s_3(B_2^2 + B_2h) - f}{d}.$$

Pela definição de D_2 temos que A_2 divide $B_2^2 + B_2h - f$, logo B' é também uma função polinomial.

- Agora mostramos que $D' = \mathrm{div}(A', B')$ é um divisor semi-reduzido. Seja

$$B' = \frac{s_1A_1B_2 + s_2A_2B_1 + s_3(B_1B_2 + f)}{d} + sA',$$

com $s \in K[X]$. Subtraindo y a cada lado temos que

$$(B' - y) = \frac{s_1A_1B_2 + s_2A_2B_1 + s_3(B_1B_2 + f) - yd}{d} + sA' = \frac{s_1A_1(B_2 - y) + s_2A_2(B_1 - y) - s_3(B_1 - y)(B_2 - y)}{d} + sA',$$

e como $(B' - y)\sigma(B' - y) = (B' - y)(B' + y + h) = B'^2 + B'h - f$, então podemos ver que para A' dividir $B'^2 + B'h - f$, é suficiente mostrar que o produto A_1A_2 divide o produto de

$$s_1A_1(B_2 - y) + s_2A_2(B_1 - y) - s_3(B_1 - y)(B_2 - y)$$

com

$$\sigma(s_1A_1(B_2 - y) + s_2A_2(B_1 - y) - s_3(B_1 - y)(B_2 - y));$$

isto é imediato, pois A_1 divide $B_1^2 + B_1h - f = (B_1 - y)\sigma(B_1 - y)$ e A_2 divide $B_2^2 + B_2h - f = (B_2 - y)\sigma(B_2 - y)$. Portanto, pela Observação (1.5) o $\mathrm{div}(A', B')$ é um divisor semi-reduzido.

- Por último, mostramos que $D' \sim D_1 + D_2$. Seja $P = (a, b) \in \mathbf{H}(L)$. Temos dois casos a considerar:

(1) Se $P \neq \sigma(P)$.

(1.a) Suponhamos que $v_P(D_1) = m_1$,$v_{\sigma(P)}(D_1) = 0$, $v_P(D_2) = m_2$ e $v_{\sigma(P)}(D_2) = 0$, onde $m_1, m_2 \geq 0$. Logo, $v_P(B_1 - y) \geq m_1$ e $v_P(B_2 - y) \geq m_2$. Se $m_1 = 0$ ou $m_2 = 0$, então $v_P(d_1) = 0$,

implicando que $v_P(d) = 0$ e $v_P(A') = m_1 + m_2$. Se $m_1, m_2 \geq 1$, então temos que $(B_1 + B_2 + h) = 2a + h(a) \neq 0$, logo $v_P(d) = 0$ e $v_P(A') = m_1 + m_2$; da equação (9) segue que

$$v_P(B' - y) \geq \min\{m_1 + m_2, m_2 + m_1, m_1 + m_2\} = m_1 + m_2.$$

Portanto, $v_P(D') = m_1 + m_2$.

(1.b) Suponha que $v_P(D_1) = m_1$ e $v_{\sigma(P)}(D_2) = m_2$, onde $m_1 \geq m_2 \geq 1$. Nós temos que $v_P(A_1) = m_1$, $v_P(a_2) = m_2$, $v_P(D_1) = m_2$, $v_P(B_1 - y) \geq m_1$, $v_P(B_2 - y) = 0$ e $v_{\sigma(P)}(B_2 - y) \geq m_2$. A última desigualdade implica que $v_P(B_2 + h + y) \geq m_2$ e daqui $v_P(B_1 + B_2 + h) \geq m_2$ ou $(B_1 + B_2 + h) = 0$. Logo, $v_P(d) = m_2$ e $v_P(A') = m_1 - m_2$. Da equação (9) temos

$$v_P(B' - y) \geq \min\{m_1 + 0, m_2 + m_1, m_1 + 0\} - m_2 = m_1 - m_2.$$

Portanto $v_P(D') = m_1 - m_2$.

(2) Se $P = \sigma(P)$.

(2.a) Suponhamos que $v_P(D_1) = 1$ e $v_P(D_2) = 1$. Então, $v_P(A_1) = 2$, $v_P(A_2) = 2$ e $v_P(d_1) = 2$. Temos que $(B_1 + B_2 + h)(a) = 2b + h(a) = 0$, logo $v_P(B_1 + B_2 + h) \geq 2$ ou $(B_1 + B_2 + h) = 0$; então $v_P(d) = 2$ e $v_P(A') = 0$. Portanto, $v_P(D') = 0$.

(2.b) Suponhamos que $v_P(D_1) = 1$ e $v_P(D_2) = 0$, logo $v_P(A_1) = 2$, $v_P(A_2) = 0$. Daqui temos $v_P(d_1) = v_P(d) = 0$ e $v_P(A') = 2$. Como $v_P(A_2) = 0$, e da equação (9) temos $v_P(B' - y) \geq 1$, da equação (9) podemos dizer que $v_P(B' - y) \geq 2$ só se $v_P(s_2A_2 + s_3(B_2 - y)) \geq 1$. Se isto acontece, então $v_P(s_2A_2 + s_3(B_2 + h + y)) \geq 1$ (ou $s_2A_2 + s_3(B_1 + B_2 + h) = 0$). Isto implica que da equação (7) $v_P(d) \geq 1$, contradição. Logo $v_P(B' - y) = 1$, e portanto $v_P(D') = 1$.

Exemplo 2.2. Consideremos a curva hiperelíptica $\mathbf{H}$ definida por $Y^2 + (X^2 + X)Y = X^5 + X^3 + 1$, de gênero 2 sobre o corpo $\mathbb{F}_{2^5} = \mathbb{F}_2[X]/(X^5 + X^2 + 1)$.

(1) Sejam $P = (\alpha^{30}, 0)$, $\sigma(P) = (\alpha^{30}, \alpha^{16})$, $Q_1 = (0, 1)$ e $Q_2 = (1, 1)$, onde α é um gerador do subgrupo multiplicativo de $\mathbb{F}_{2^5}$. Definamos os divisores reduzidos $D_1 = P + Q_1 - 2\mathcal{O}$ e $D_2 = \sigma(P) + Q_2 - 2\mathcal{O}$. Primeiro achamos os polinômios $A_1, B_1, A_2, B_2 \in \mathbb{F}_{2^5}[X]$ tais que $D_1 = \text{div}(A_1, B_1)$ e $D_2 = \text{div}(A_2, B_2)$. Então temos que $A_1 =$

$\prod_{P\in \sup(D_1)}(X-a_P)^{v_P(D_1)}$, logo $A_1 = X(X+\alpha^{30})$. Usando as condições do lema (1.4), obtemos $B_1 = \alpha X + 1$. Análogamente, temos que $A_2 = (X+\alpha^{30})(X+1)$ e $B_2 = \alpha^{23}X + \alpha^{12}$. A seguir, aplicamos o Algoritmo (1) para achar o divisor semi-reduzido equivalente à soma de D_1 e D_2. Logo, calculamos $d_1 = \mathrm{mdc}(A_1, A_2) = X + \alpha^{30}$ tal que

$$d_1 = A_1 + A_2 \quad \text{e} \quad d = \mathrm{mdc}(d_1, B_1 + B_2 + h) = X + \alpha^{30},$$

assim $d = d_1$. Então,

$$A' = A_1A_2/d^2 = X(X+1), \qquad \text{e} \qquad B' \equiv 1 \pmod{A'}.$$

Dos polinômios acima, segue-se

$$\mathrm{div}(A') = 2Q_1 + 2Q_2 - 4\mathcal{O}$$

e

$$\mathrm{div}(B' - y) = \mathrm{div}(y+1) = Q_1 + Q_2 + \sum_{i=1}^{3} P_i - 5\mathcal{O},$$

onde $P_i \neq Q_1, Q_2$. Portanto, $D' = \mathrm{div}(A', B') = Q_1 + Q_2 - 2\mathcal{O}$.

(2) Sejam $D_1 = P + Q_1 - 2\mathcal{O}$ e $D_2 = Q_1 + Q_2 - 2\mathcal{O}$. Então $D_1 = \mathrm{div}(A_1, B_1)$ e $D_2 = \mathrm{div}(A_2, B_2)$ onde $A_1 = X(X+\alpha^{30})$, $B_1 = \alpha X + 1$, $A_2 = X(X+1)$ e $B_2 = 1$. Logo, como $d = d_1 = X$, obtemos

$$A' = (X+\alpha^{30})(X+1), \qquad \text{e} \qquad B' \equiv \alpha^{14}X + \alpha^{13} \pmod{A'}.$$

Daqui,

$$\mathrm{div}(A') = 2Q_2 + P + \sigma(P) - 4\mathcal{O}$$

e

$$\mathrm{div}(B' - y) = Q_2 + P + \sum_{i=1}^{3} P_i - 5\mathcal{O}, \quad \text{tal que} \quad P_i \neq Q_2, P, \sigma(P),$$

portanto, $D' = \mathrm{div}(A', B') = Q_2 + P - 2\mathcal{O}$.

Algoritmo 2. Seja $D' = \mathrm{div}(A', B')$ um divisor semi-reduzido; o procedimento a seguir acha um divisor $D = \mathrm{div}(A, B)$ reduzido e equivalente a D' tal que $\deg(A) < \deg(A')$. Aplicando sucessivamente este algoritmo, achamos um divisor reduzido $\widetilde{D} = \mathrm{div}(\widetilde{a}, \widetilde{b})$ equivalente a D' tais que $\deg\widetilde{a} \leq g$. Então,

$$A = (f - hb - b^2)/A' \tag{10}$$

e

$$B = (-h - B) \pmod{A}; \tag{11}$$

se c é o coeficiente líder de A, então $A = c^{-1}A$. A seguir, mostramos que o Algoritmo (2) devolve um divisor equivalente a D' e de menor grau.

(1) Mostremos que $\deg(A) \leq \deg(A')$. Seja $m = \deg(A')$, e $n = \deg(B')$, onde $m > n$ e $m \geq g + 1$. Logo $\deg(A) = \max\{2g + 1, 2n\} - m$. Se $m = g + 1$, então $\deg(A) = g < \deg(A')$. Se $m > g + 1$, então $\max\{2g + 1, 2n\} \leq 2(m - 1)$, logo $\deg(A) \leq (m - 2) \leq \deg(A')$.

(2) $D = \mathrm{div}(A, B)$ é um divisor semi-reduzido. De (10) $f - B'h - B'^2 = AA'$, então passando módulo A a ambos lados e aplicando (11) temos que

$$f + (B + h)h - (B + h)^2 \equiv 0 \pmod{A}.$$

Simplificando fica $f - Bh - B^2 \equiv 0 \pmod{A}$. Portanto A divide $(f - Bh - B^2)$, e aplicando o Lema 1.4 concluímos que $D = \mathrm{div}(A, B)$ é um divisor semi-reduzido.

(3) Escrevamos o divisor D' da seguinte forma:

$$D' = \sum_{P \neq \sigma(P)} n_P P + \sum_{P = \sigma(P)} P - m\mathcal{O}.$$

Pela prova do lema (1.4) podemos escrever

$$\mathrm{div}(A') = \sum_{P \neq \sigma(P)} n_P P + \sum_{P \neq \sigma(P)} n_P \sigma(P) + \sum_{P = \sigma(P)} 2P - (*)\mathcal{O}\,,$$

$$\mathrm{div}(B' - y) = \sum_{P \neq \sigma(P)} m_P P + \sum_{P = \sigma(P)} P + \sum_{P \in \mathbf{H}'} s_P P - (*)\mathcal{O}\,,$$

onde $m_P \geq n_P$, $s_P \geq 1$ e $\mathbf{H}' = \mathbf{H} \backslash (\mathrm{sup}(D') \cup \{\sigma(P) : P \in \mathrm{sup}(D')\} \cup \{\mathcal{O}\})$. Como $(B'^2 + B'h - f) = (B' - y)(B' + y + h)$, temos que

$$\mathrm{div}(B'^2 + B'h - f) = \sum_{P \neq \sigma(P)} m_P P + \sum_{P \neq \sigma(P)} m_P \sigma(P) + \sum_{P = \sigma(P)} 2P + \sum_{P \in \mathbf{H}'} s_P P + \sum_{P \in \mathbf{H}'} s_P \sigma(P) - (*)\mathcal{O}\,;$$

assim, usando a equação (10) temos

$$\begin{aligned}\operatorname{div}(A) &= \operatorname{div}(B'^2 + B'h - f) - \operatorname{div}(A') = \\ &= \sum_{P\neq\sigma(P)} t_P P + \sum_{P\neq\sigma(P)} t_P\sigma(P) + \sum_{P\in\mathbf{H}'} s_P P + \sum_{P\in\mathbf{H}'} s_P\sigma(P) - (*)\mathcal{O}\,,\end{aligned}$$

onde $t_P = m_P - n_P$. Como $B = -h - B' + sA$, onde $s \in \mathcal{K}[X]$, para $P = (a, b) \in \sup(\operatorname{div}(A))$, temos que $B(a) = -h(a) - B'(a) + s(a)A(a) = -h(a) - b$. Então

$$\operatorname{div}(B - y) = \sum_{P\neq\sigma(P)} r_P\sigma(P) + \sum_{P\in\mathbf{H}'} w_P\sigma(P) + \sum_{P\in\widetilde{\mathbf{H}}} z_P P - (*)\mathcal{O}\,,$$

onde $r_P \geq t_P$, $w_P \geq s_P$ e $\widetilde{\mathbf{H}}$ é o conjunto $\mathbf{H}\setminus\sup(\operatorname{div}(B-y))$. Logo,

$$\begin{aligned}\operatorname{div}(A, B) &= \sum_{P\neq\sigma(P)} t_P\sigma(P) + \sum_{P\in\mathbf{H}'} s_P\sigma(P) - (*)\mathcal{O} \\ &\sim -\sum_{P\neq\sigma(P)} t_P P - \sum_{P\in\mathbf{H}'} s_P P - (*)\mathcal{O} \\ &= D - \operatorname{div}(B' - y)\,.\end{aligned}$$

Portanto $D \sim D'$. Notemos que o divisor $D = \operatorname{div}(A, B)$ é reduzido se e somente se $\deg(A) \leq g$, onde g é o gênero da curva.

Exemplo 2.3. Seja a curva $H : Y^2 + (X^2 + X)Y = X^5 + X^3 + 1$ de gênero 2 definida sobre $\mathbb{F}_{2^5}$. Consideremos o divisor semi-reduzido $D' = (0, 1) + (1, 1) + (\alpha^5, \alpha^{15}) - 3\mathcal{O}$. Então $D' = \operatorname{div}(A', B')$, onde $A' = X(X + 1)(X + \alpha^5)$ e $B' = \alpha^{17}X^2 + \alpha^{17}X + 1$. Agora, calculamos os polinômios A e B tais que $D = \operatorname{div}(A, B)$ é o divisor reduzido equivalente a D'. Então,

$$A = (X + \alpha^{28})(X + \alpha^{29})\,, \text{e}\, B \equiv \alpha^{23}X + \alpha^{21} \pmod{A}\,.$$

Logo,

$$\operatorname{div}(A) = (\alpha^{28}, \alpha^7) + (\alpha^{28}, \alpha^{16}) + (\alpha^{29}, 0) + (\alpha^{29}, \alpha) - 4\mathcal{O}$$

e,

$$\operatorname{div}(B + y) = (\alpha^{28}, \alpha^7) + (\alpha^{29}, 0) + \sum_{i=1}^{3} P_i - 5\mathcal{O}\,.$$

Portanto $D = \operatorname{div}(A, B) = (\alpha^{28}, \alpha^7) + (\alpha^{29}, 0) - 2\mathcal{O}$.

Exemplo 2.4. Considerando a curva **H** definida por

$$Y^2 + XY = X^5 + 5X^4 = 6X^2 + X + 3,$$

de gênero 2 sobre o corpo $\mathbb{F}_7$, seja o divisor semi-reduzido

$$D' = \operatorname{div}(A', B') = \operatorname{div}(X^7 + 2X^6 + 3X^5 + 6X^3 + 4X + 5, \\ 5X^6 + 5X^5 + 6X^4 + 4X^3 + 5X^2 + 4).$$

Achemos o divisor reduzido D equivalente a D'. Aplicando o Algoritmo (2) a D' obtemos o divisor

$$D'_1 = \operatorname{div}(A'_1, B'_1) = \operatorname{div}(x^5 + 6x^3 + 6x^2 + 6x + 1, 3x^4 + 6x^2 + 6x + 1).$$

Como o grau de A'_1 e $5 \geq g = 2$ o gênero da curva, então continuamos aplicando o algoritmo até ter um divisor reduzido. Assim,

$$D = \operatorname{div}(A, B) = \operatorname{div}(x^2 + x + 5, 4x + 4)\,.$$

3. Criptossistemas usando curvas hiperelípticas

A implementação de novos grupos em criptossistemas de chave pública que baseiam a segurança no problema do logaritmo discreto (por exemplo, Diffie-Hellman e ElGamal) é cada vez mais importante para lograr um nível maior de segurança. O Jacobiano de curvas hiperelípticas é um grupo com as características adequadas para aplicar na criptografia baseado também na intratabilidade deste problema.

Definição 3.1. O Problema do logaritmo Discreto sobre o Jacobiano de Curvas Hiperelípticas $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_{q^n})$ (HECDLP) é definido, dados dois divisores D_1 e D_2 sobre $\mathbb{F}_{q^n}$, como o problema de determinar um inteiro m, se existe, tal que $[D_2] = m[D_1]$ em $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_{q^n})$, ou equivalentemente, $mD_1 - D_2 \in P_{\mathbf{H}}(\mathbb{F}_{q^n})$.

Assim, podemos definir em forma natural o sistema de troca de chaves Diffie-Hellman entre os usuários **A** e **B**, sobre o Jacobiano de uma curva hiperelíptica definida em um corpo finito. Os parâmetros públicos são: o corpo finito $\mathbb{F}_q^n$, a equação da curva hiperelíptica **H** e um elemento base $D_0 \in \mathcal{J}_{\mathbf{H}}(\mathbb{F}_{q^n})$. **A** escolhe um inteiro $m_{\mathbf{A}}$, sua chave privada e envia para **B** o ponto $m_{\mathbf{A}}D_0$; análogamente, **B** envia $m_{\mathbf{B}}D_0$, onde **B** é sua chave privada. Logo o segredo compartilhado será o divisor $m_{\mathbf{A}}m_{\mathbf{B}}D_0 \in \mathcal{J}_{\mathbf{H}}(\mathbb{F}_{q^n})$.

Uma condição importante para a escolha de uma curva hiperelíptica está relacionada com a dificuldade de resolver o problema do logaritmo discreto sobre seu Jacobiano. Assim, a seguir mostramos o ataque Index-Calculus para o problema do logaritmo discreto.

3.8. Ataque Index-Calculus para resolver o HECDLP

O Index-Calculus [7] tem sido aplicado satisfatoriamente em vários problemas criptográficos interessantes, incluindo o DLP para corpos finitos. Esta mesma ideia pode ser usada para o DLP no Jacobiano $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_{q^n})$ de uma curva hiperelíptica $\mathbf{H}$ de gênero g definida sobre $K = \mathbb{F}_q$. No que segue, $D_1 \in \mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$, $D_2 \in [D_1]$, e queremos determinar m tal que $[D_2] = m[D_1]$ ou $m = \log_{D_1} D_2$. **(1)** O primeiro passo é computar a estrutura de $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$ como soma direta de subgrupos cíclicos, e se procurão representações de D_1 e D_2 sobre esta soma direta; logo para resolver o DLP simplesmente aplicamos o Teorema Chinês dos Restos Generalizado. Para descrever o método, introduzimos algumas definições.

Definição 3.2. Seja $D = \mathrm{div}(A, B)$ um divisor semi-reduzido sobre $\mathbf{H}$. Dizemos que D é um divisor *primo* se o polinômio A é irredutível sobre $\mathbb{F}_q$, o corpo base de $\mathbf{H}$.

Seja $A \in K[X]$ um polinômio irredutítivel e α uma raiz de A. Dizemos que $Y^2 + h(X)Y - f(X)$ é separável $\pmod A$, se $Y^2 + h(\alpha)Y - f(\alpha)$ tem duas raízes distintas em $K(\alpha)$.

Definição 3.3. O polinômio A é dito separável se A não divide $f(X)$ e $Y^2 + h(X)Y - f(X)$ é separável $\pmod A$.

Definição 3.4. O polinômio A é dito ramificado se A divide f.

Chamamos um primo $r_P \in K(\mathbf{H})$ separável ou ramificado respectivamente, se este está sobre $A \in K(X)$ que é separável ou ramificado. Para $D \in \mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$ tal que $D = \mathrm{div}(A, B)$, podemos escrever este como a soma de divisores primos da forma $D_i = \mathrm{div}(A_i, B_i)$, onde os A_i são fatores primos de A. Seja t um inteiro chamado a cota de *smoothness*.

Definição 3.5. Um divisor é dito t-smooth se todos seus divisores primos são de grau menor ou igual a t.

Quando $t = 1$, um divisor 1-smooth será um divisor para o qual o polinômio A é completamente separável sobre $\mathbb{F}_q$.

Seja $S = \{P_1, \ldots, P_n\}$ a *base fator* onde $P_i = \mathrm{div}(A_i, B_i)$ são todos os divisores primos ramificados e separáveis tal que $\deg(A_i) \leq t$ para algum $t \in \mathbb{Z}$. Se A_i é sepáravel, então unicamente um dos divisores primos sobre A_i, $\mathrm{div}(A_i, B_i)$ ou $\mathrm{div}(A_i, -B_i - h)$, está em S.

O primeiro passo do algoritmo é achar $m > n$, t-smooth divisores principais tal que se tenha a relação $\sum_j \alpha_j P_j \sim \mathcal{O}$. Se S gera $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$, então a aplicação

$$\phi : \mathbb{Z}^n \to \mathcal{J}_{\mathbf{H}}(\mathbb{F}_q) \quad \text{onde} \quad \phi(\alpha_1, \ldots, \alpha_n) \mapsto \sum_j \alpha_j P_j$$

é um homomorfismo sobrejetivo, logo $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q) \cong \mathbb{Z}^n/\mathrm{Ker}(\phi)$. Cada relação é um elemento $\alpha_i' = (\alpha_{i1}, \ldots, \alpha_{in}) \in \mathrm{Ker}(\phi)$, e se o conjunto de m relações forma um sistema completo de geradores do $\mathrm{Ker}(\phi)$, então

$$\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q) \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_n\mathbb{Z}$$

tal que $(d_1, \ldots, d_n)$ são os elementos da *forma normal de Smith* (SNF) da matriz relação $A = (\alpha_1' \ldots \alpha_m')$ onde os α_i estão escritos como colunas. Geradores X_i de cada subgrupo $\mathbb{Z}/d_i\mathbb{Z}$ podem ser calculados achando as matrizes $T = (T_{ij})$ e $Q = (Q_{ij})$ tal que $T^{-1}AQ = SNF(A)$, e fazemos $X_i = \sum_{j=1}^{n} T_{ij} P_j$.

O segundo passo do algoritmo é achar representações de D_1 e D_2 em $Z/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_n\mathbb{Z}$. Se D_1 e D_2 podem ser fatorados sobre S como $D_1 \sim \sum r_i P_i$ e $D_2 \sim \sum s_i P_i$, então podemos escolher $D_1 = \sum r_i' X_i$ e $D_2 = \sum s_i' X_i$ onde $(r_1', \ldots, r_n') = P^{-1}(r_1, \ldots, r_n)^T$ e $(s_1', \ldots, s_n') = P^{-1}(s_1, \ldots, s_n)^T$. Assim, obtemos as representações de $D_1 = (r_1', \ldots, r_n')$ e $D_2 = (s_1', \ldots, s_n')$ em $\mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_n\mathbb{Z}$, logo o DLP pode ser resolvido usando o Teorema Chinês dos Restos generalizado para achar $m \in \mathbb{Z}$ tal que as congruências $r_i' \equiv m s_i' \pmod{d_i}$, onde $1 \leq i \leq n$, sejam simultaneamente satisfeitas.

(2) O segundo método melhora o primeiro quando $\#\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$ é conhecido. Como acima, seja $S = \{P_1, \ldots, P_n\}$ a base fator com todos os divisores primos de grau menor o igual que t. As relações são achadas por tentativas para fatorar divisores da forma $rD_1 + sD_2$ sobre S. Cada divisor t-smooth leva a uma relação da forma $r_i D_1 + s_i D_2 \sim Q_i = \sum_j \alpha_{ij} P_j$. Quando tem sido achados $n+1$ relações diferentes, aplicamos o módulo $\#\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$ para encontrar uma combinação linear não trivial da forma $\sum_{i=1}^{n+1} \gamma_i \alpha_i' = (0, \ldots, 0)$, o qual implica que $\sum_{i=1}^{n+1} \gamma_i Q_i = 0$. Logo, $\sum_{i=1}^{n+1} \gamma_i (r_i D_1 + s_i D_2) = 0$ e $\log_{D_1} D_2 = -(\sum \gamma_i r_i)/(\sum \gamma_i s_i) \pmod{\#\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)}$.

Referenzas

[1] I. BLAKE, G. SEROUSSI, N. SMART. "Elliptic Curves in Cryptgraphy". *London Mathematical Society Lecture Note series*, 265, Cambrigde, 1999.

[2] D. CANTOR. "Computing in the jacobian of a hiperelliptic curve". *Math. Comp.* **4**8, 95–101, 1987.

[3] W. FULTON. *Algebric Curves.* Benjamin, New York, 1969.

[4] N. KOBLITZ. "Hyperelliptic cryptosystems". *Journal Criptology 1*, 139–150, 1989.

[5] N. KOBLITZ. *Algebraic Aspects of Cryptography.* Springer-Verlag, Berlin-Heidelberg-New York, 1998.

[6] H. STICHTENOTH. *Algebraic Function Fields and Codes.* Springer-Verlag, Berlin, Heidelberg, 1993.

[7] N. THÉRIAULT. "Index Calculus attack for hyperellíptic curves os small genus", 2003. (http://www.math.toronto.edu/ganita/publications.html)

ALONSO SEPÚLVEDA CASTELLANOS
Bolsista do Cnpq
Instituto de Matemática, Estatistica e Computação Cientifica IMECC
Unicamp-Brasil.
e-mail: alonsosc@ime.unicamp.br