Применение альтернативных моделей эллиптических кривых в криптографии на основе изогений

С. Гребнев[1], А. Тулебаев[2]

[1]QApp [2]Код безопасности

RusCrypto’2021, Москва

Изогении

Изогения — это рациональное отображение между двумя эллиптическими кривыми, являющееся гомоморфизмом. Если существует такого рода отображение между двумя кривыми, то они называются **изогенными**.
Сложность вычисления изогении степени l (т.е. с ядром мощностью l) есть $O(l)$ операций в поле $GF(p^2)$ (при помощи **формул Велю**).
При этом для вычисления изогении гладкой степени можно воспользоваться ее декомпозицией на изогении малых степеней.

Формулы Велю

Пусть $y^2 = x^3 + ax + b$ – эллиптическая кривая над полем K. Пусть F – подгруппа E(K) порядка l. Тогда изогения с ядром F строится по следующему алгоритму.

1. Разобьем $F \setminus \{\mathcal{O}\}$ на три непересекающихся множества, $F = F_2 \cup R_+ \cup R_-$, где F_2 – множество точек четного порядка, а R_+ и R_- – разбиение множества точек нечетного порядка так, что $R \in R_+$ тогда и только тогда, когда $-R \in R_-$.
2. Определим множество S: $S = F_2 \cup R_+$.
3. Для каждой точки $Q \in S$ будем вычислять $g_Q^x = 3x^2 x_Q + a$, $g_Q^y = -2y_Q$ (здесь (x_Q, y_Q) – координаты точки Q); если $Q = -Q$, то $v_Q = g_Q^x$, иначе $v_Q = 2g_Q^x$; $u_Q = (g_Q^x)^2$
4. Вычислим $v = \sum_{Q\in S} v_Q$; $w = \sum_{Q \in S}(u_Q + x_Q v_Q)$.
5. Коэффициенты изогенной кривой определяются как
$$a' = a - 5v;$$
$$b' = b - 7w.$$
6. Формулы преобразования координат $(x, y) \mapsto (x', y')$ имеют вид
$$x' = x + \sum_{Q\in S}\left(\frac{v_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2}\right),$$
$$y' = y + \sum_{Q\in S}\left(u_Q \frac{2y}{(x - x_Q)^3} + v_Q \frac{y - y_Q}{(x - x_Q)^2} - \frac{g_Q^x g_Q^y}{(x - x_Q)^2}\right).$$

Протокол SIDH

В основе протокола лежит следующая коммутативная диаграмма:

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[d, "\psi"'] & E/\langle P\rangle \arrow[d] \\ E/\langle Q\rangle \arrow[r] & E/\langle P, Q\rangle \end{tikzcd} \tag{1}$$

где φ, ψ – случайные пути в графах изогений степеней 2^{e_A}, 3^{e_B} соответственно.
Таким образом, нас интересуют эффективные аналоги формул Велю для степеней 2, 3 и 4.

Формулы Велю для 2- и 3-изогений

2-изогении
Пусть $\mathsf{P} = (\mathsf{x_P}, 0)$ – точка порядка 2 на $\mathsf{E_{a,b}}(\mathsf{GF}(\mathsf{p}^2))$. Положим $\mathsf{v} = 3\mathsf{x_P^2} + \mathsf{a}$, $\mathsf{a}' = \mathsf{a} - 5\mathsf{v}$, $\mathsf{b}' = \mathsf{b} - 7\mathsf{v}\mathsf{x_P}$; тогда отображение

$$(\mathsf{x}, \mathsf{y}) \mapsto \left(\mathsf{x} + \frac{\mathsf{v}}{\mathsf{x} - \mathsf{x_P}}, \mathsf{y} - \frac{\mathsf{vy}}{(\mathsf{x} - \mathsf{x_P})^2}\right)$$

задает 2-изогению из $\mathsf{E_{a,b}}$ в $\mathsf{E_{a',b'}}$ с ядром $\langle \mathsf{P} \rangle$.

Формулы Велю для 2- и 3-изогений

3-изогении

Пусть $P = (x_P, y_P)$ – точка порядка 3 на $E_{a,b}(GF(p^2))$. Положим $v = 2(3x_P^2 + a)$, $u = 4y_P^2$, $a' = a - 5v$, $b' = b - 7(u + vx_P)$; тогда отображение

$$(x, y) \mapsto \left(x + \frac{v}{x - x_P} + \frac{u}{(x - x_P)^2}, y\left(1 - \frac{v}{(x - x_P)^2} - \frac{2u}{(x - x_P)^3}\right)\right)$$

задает 3-изогению из $E_{a,b}$ в $E_{a',b'}$ с ядром $\langle P \rangle$.

Кривые Монтгомери

Кривая Монтгомери задается уравнением

$$M_{A,B}(GF(p)) : By^2 = x^3 + Ax^2 + x, \text{ где } B(A^2 - 4) \neq 0. \qquad (2)$$

Пусть $m > n > 0$, $P = (X_1 : Y_1 : Z_1) \in M_{A,B}$, известны кратные точки $P_n = nP$, $P_m = mP$, $P_{m-n} = (m-n)P$. Тогда имеют место формулы

$$X_{m+n} = Z_{m-n}((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n))^2$$
$$Z_{m+n} = X_{m-n}((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n))^2$$

$$4X_nZ_n = (X - n + Z_n)^2 - (X_n - Z_n)^2$$
$$X_{2n} = X - n + Z_n)^2(X_n - Z_n)^2$$
$$Z_{2n} = 4X_nZ_n((X_n - Z_n)^2 + ((A+2)/4)(4X_nZ_n))$$

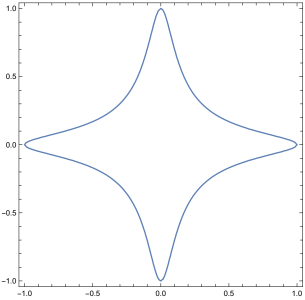
Кривые Монтгомери

Эффективная арифметика в XZ–проективных координатах

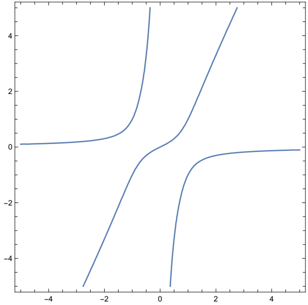
Алгоритм	Сложность
Сложение	$5\mathsf{M} + 2\mathsf{S}$
Удвоение	$3\mathsf{M} + 2\mathsf{S}$
Утроение	$8\mathsf{M} + 4\mathsf{S}$

(C. Costello, B. Smith, 2017)

Кривые Эдвардса и Хаффа



$$x^2 + y^2 = c^2(1 + dx^2y^2)$$



$$ax(y^2 - 1) = by(x^2 - 1)$$

Проективные координаты Эдвардса

Точка (x, y) на кривой Эдвардса представляется в виде тройки $(X : Y : Z)$ такой, что $(X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$, $(x, y) = (X/Z, Y/Z)$. Нейтральный элемент группы точек имеет координаты $(0 : 1 : 1)$. Обратным элементом к точке $(X : Y : Z)$ является точка $(-X : Y : Z)$.

Алгоритм	Сложность
Сложение	$10M + 1S + 1 * c + 1 * d$
Удвоение	$3M + 4S + 3 * c$
Утроение	$9M + 4S + 1 * c$

(http://hyperelliptic.org/EFD/)

w-координаты Хаффа

Вводится рациональная функция $w(x, y) = \frac{1}{xy}$; $c = a/b$;

$$w_{2P} = \frac{(w_P^2 - 1)^2}{4w_P(w_P + c)(w_P + 1/c)}$$

$$w_{P+Q} = \frac{(w_P w_Q - 1)^2}{(w_P - w_Q)w_{P-Q}}$$

В проективных $w-$координатах имеем

Алгоритм	Сложность
Сложение	$3M + 2S$
Удвоение	$2M + 2S + C$
Утроение	$7M + 5S$

(Huang Y., Zhang F., Hu Z., Liu Z., 2020)

Кривые Монтгомери

2-изогении
Пусть R – точка порядка 2 на кривой $M_{A,B}$, $x_R \neq 0$, и пусть $\phi_2 : M_{A,B} \to M_{A',B'}$ — единственная (с точностью до изоморфизма) 2-изогения с ядром $\langle R\rangle$, тогда параметры кривой $M_{A',B'}$ вычисляются по формуле

$$(A', B') = \left(2 \cdot (1 - 2x_R^2), Bx_R\right). \tag{3}$$

Если Q – точка на кривой $M_{A,B}$, $Q \notin \ker(\phi_2)$, то ее образ $Q' = \phi_2(Q) \in M_{A',B'}$ вычисляется как

$$\begin{aligned} x_{Q'} &= \frac{x_Q^2 x_R - x_Q}{x_Q - x_R}, \\ y_{Q'} &= y_Q \cdot \frac{x_Q^2 x_R - 2x_Q x_R^2 + x_R}{(x_Q - x_R)^2}. \end{aligned} \tag{4}$$

4-изогении
Пусть R – точка порядка 4 на кривой $M_{A,B}$, $x_R \neq \pm 1$, и пусть $\phi_4 : M_{A,B} \to M_{A',B'}$ — единственная (с точностью до изоморфизма) 4-изогения с ядром $\langle R\rangle$, тогда параметры кривой $M_{A',B'}$ вычисляются по формуле

$$(A', B') = \left(4x_R^4 - 2, -x_R(x_R^2 + 1) \cdot B/2\right). \tag{5}$$

Если Q – точка на кривой $M_{A,B}$, $Q \notin \ker(\phi_4)$, то ее образ $Q' = \phi_4(Q) \in M_{A',B'}$ вычисляется как

Кривые Монтгомери

$$x_{Q'} = \frac{-(x_Q x_R^2 + x_Q - 2x_R)x_Q(x_Q x_R - 1)^2}{(x_Q - x_R)^4(2x_Q x_R - x_R^4 - 1)},$$

$$y_{Q'} = y_Q \cdot \frac{-2x_R^2(x_Q x_R - 1)x_Q^4(x_R^2 + 1) - 4x_Q^3(x_R^3 + x_R) + 2x_Q^2(x_R^4 + 5x_R^2) - 4x_Q(x_R^3 + x_R) + x_R^2 + 1}{(x_Q - x_R)^3(2x_Q x_R - x_R^4 - 1)^2}. \tag{6}$$

3-изогении

Пусть R – точка порядка 3 на кривой $M_{A,B}$, и пусть $\phi_3 : M_{A,B} \to M_{A',B'}$ — единственная (с точностью до изоморфизма) 3-изогения с ядром $\langle R \rangle$, тогда параметры кривой $M_{A',B'}$ вычисляются по формуле

$$(A', B') = \left((Ax_R - 6x_R^2 + 6)x_R, Bx_R^2\right). \tag{7}$$

Если Q – точка на кривой $M_{A,B}$, $Q \notin \ker(\phi_3)$, то ее образ $Q' = \phi_3(Q) \in M_{A',B'}$ вычисляется как

$$x_{Q'} = \frac{x_Q(x_Q x_R - 1)^2}{(x_Q - x_R)^2},$$

$$y_{Q'} = y_Q \cdot \frac{(x_Q x_R - 1)(x_Q^2 x_R - 3x_Q x_R^2 + x_Q + x_R)}{(x_Q - x_R)^3}. \tag{8}$$

Кривые Эдвардса

Пусть E_d – кривая Эдвардса над полем K, γ, δ, i – элементы K либо его алгебраического расширения такие, что $\gamma^2 = 1 - d$, $\delta^2 = d$, $i^2 = -1$. Тогда существуют 2-изогении с кривой E_d, заданные отображениями ψ_1, ψ_2, ψ_3:

$$\psi_1 : (x, y) \mapsto \left((\gamma \mp 1)xy, \frac{(\gamma \mp 1)y^2 \pm 1}{(\gamma \mp 1)y^2 \mp 1} \right). \tag{9}$$

Образ кривой E_d при этом отображении задается уравнением

$$E_{\hat{d}} : x^2 + y^2 = 1 + \hat{d}x^2y^2 \tag{10}$$

при $\hat{d} = \left(\frac{\gamma \pm 1}{\gamma \mp 1}\right)^2$.

$$\psi_2 : (x, y) \mapsto \left((i\gamma \pm \delta)\frac{x}{y}, -\frac{\delta y^2 \mp i\gamma - \delta}{\delta y^2 \pm i\gamma - \delta} \right). \tag{11}$$

Образ кривой E_d при этом отображении задается уравнением

$$E_{\hat{d}} : x^2 + y^2 = 1 + \hat{d}x^2y^2 \tag{12}$$

при $\hat{d} = \left(\frac{i\gamma \mp \delta}{i\gamma \pm \delta}\right)^2$.

$$\psi_3 : (x, y) \mapsto \left((i\delta \mp 1)\frac{x}{y}\frac{1 - dy^2}{1 - d}, \frac{d \mp \delta}{d \pm \delta}\frac{\delta y^2 \pm 1}{\delta y^2 \mp 1} \right). \tag{13}$$

Кривые Эдвардса

Образ кривой E_d при этом отображении задается уравнением

$$E_{\hat{d}} : x^2 + y^2 = 1 + \hat{d}x^2y^2 \tag{14}$$

при $\hat{d} = \left(\frac{\delta \pm 1}{\delta \mp 1}\right)^2$.
Вычисление 2-изогенной кривой Эдвардса требует вычисления квадратного корня в поле, однако, этого можно избежать, используя 4-изогении.

Кривые Эдвардса

Пусть F – подгруппа кривой Эдвардса нечетного порядка $l = 2s + 1$,

$$F = \{(0, 1), (\pm\alpha_1, \beta_1), \ldots, (\pm\alpha_s, \beta_s)\}.$$

Положим

$$\psi(P) = \left(\prod_{Q \in F} \frac{x_{P+Q}}{y_Q}, \prod_{Q \in F} \frac{y_{P+Q}}{y_Q} \right).$$

Тогда ψ – l-изогения с ядром F, отображающая кривую E_d в $E_{\hat{d}}$, при $\hat{d} = B^8 d^l$, $B = \prod_{i=1}^{s} \beta_i$. Также при этом имеем

$$\psi(x, y) = \left(\frac{x}{B^2} \prod_{i=1}^{s} \frac{\beta_i^2 x^2 - \alpha_i^2 y^2}{1 - d^2 \alpha^2 \beta^2 x^2 y^2}, \frac{y}{B^2} \prod_{i=1}^{s} \frac{\beta_i^2 y^2 - \alpha_i^2 x^2}{1 - d^2 \alpha^2 \beta^2 x^2 y^2} \right). \qquad (15)$$

Кривые Хаффа

Пусть F – подгруппа кривой Хаффа $H_{a,b} : ax(y^2 - 1) = by(x^2 - 1)$ нечетного порядка $l = 2s + 1$,

$$F = \{(0,0), (\alpha_1, \beta_1), (-\alpha_1, -\beta_1) \cdots : i = 1, \dots, s\},$$

$A = \prod_{i=1}^{s} \alpha_i$, $B = \prod_{i=1}^{s} \beta_i$. Положим

$$\psi(P) = \left(x_P \prod_{Q \in F, Q \neq (0,0)} \frac{-x_{P+Q}}{x_Q}, y_P \prod_{Q \in F, Q \neq (0,0)} \frac{-y_{P+Q}}{y_Q} \right).$$

Тогда ψ – l-изогения с ядром F, отображающая кривую $H_{a,b}$ в $H_{\hat{a},\hat{b}}$ при $\hat{a} = a^l B^4$, $\hat{b} = b^l B^4$. Также при этом имеем

$$\psi(x, y) = \left(\frac{x}{A^2} \prod_{i=1}^{s} \frac{\alpha_i^2 - x^2}{1 - b^2 \alpha_i^2 x^2}, \frac{y}{B^2} \prod_{i=1}^{s} \frac{\beta_i^2 - y^2}{1 - a^2 \beta_i^2 y^2} \right). \tag{16}$$

Эта формула верна для точек, не являющихся бесконечно удаленными.
Пусть $\eta \in \overline{K}$ – такой элемент, что $\eta^2 = ab$. Тогда 2-изогения кривой Хаффа $H_{a,b}$ в $H_{\hat{a},\hat{b}}$ при $\hat{a} = -(a + 2\eta + b)$, $\hat{b} = -(a - 2\eta + b)$ задается как

$$(x, y) \mapsto \left(\frac{bx - ay}{(b-a)^2} \frac{((bx - ay) + \eta(x - y))^2}{bx^2 - ay^2}, \frac{bx - ay}{(b-a)^2} \frac{((bx - ay) - \eta(x - y))^2}{bx^2 - ay^2} \right).$$

QApp КОД безопасности

Выводы

	Модель		
	Монтгомери	Эдвардса	Хаффа
3-изогенная кривая	$2M + 3S$	$4M + 2S$	$2M + 3S$
3-изогения	$4M + 2S$	$5M + 4S$	$4M + 2S$
4-изогенная кривая	$4S$	$4M + 3S$	$4S$
4-изогения	$6M + 2S$	$6M + 2S$	$6M + 2S$

Спасибо за внимание.

sg@qapp.tech
a.tulebaev@securitycode.ru