Обращение спариваний для решения задачи дискретного логарифмирования*

М. А. ЧЕРЕПНЁВ
Московский государственный университет им. М. В. Ломоносова
e-mail: cherepniov@gmail.com

УДК 512.624

Ключевые слова: эллиптические кривые, спаривание, дискретное логарифмирование, задача Диффи—Хеллмана.

Аннотация

В статье предлагается алгоритм обращения спариваний. Эта техника может быть использована для взлома протокола Диффи—Хеллмана на эллиптических кривых и для дискретного логарифмирования на некоторых кривых, удовлетворяющих стандарту ГОСТ Р34.10-2012.

Abstract

M. A. Cherepniov, Pairing inversion for finding discrete logarithms, Fundamentalnaya i prikladnaya matematika, vol. 18 (2013), no. 4, pp. 185—195.

This paper proposes an inversion algorithm for pairings. This technique can be used for breaking the Diffie—Hellman protocol on elliptic curves and for solving the discrete logarithm problem on some curves that satisfy GOST P.34.10-2012.

1. Введение

Пусть используемая циклическая группа точек $\langle P\rangle$ кривой имеет простой порядок p. Пусть

$$p-1=\prod_{i=1}^{t} {q_i}^{\alpha_i}.$$

В стандарте ГОСТ Р34.10-2012 не указано никаких требований на это разложение, поэтому мы будем считать его имеющим общий вид. А именно, пусть

$$\psi(x,y)=\#\{1\leqslant n\leqslant x \mid \text{для любого } q, \text{ простого делителя } n, \text{ имеем } q<y\}.$$

*Работа поддержана грантом офи м2 13-01-12420.

Фундаментальная и прикладная математика, 2013, том 18, № 4, с. 185—195.

Тогда при фиксированном $u \geqslant 3$ и $x \geqslant 1$

$$\psi(x, \sqrt[u]{x}) \geqslant \frac{x}{u^{u(1+o(1))}} \tag{1}$$

[3, теорема 3.1]. Таким образом, с вероятностью, равной константе, можно считать, что $q_i \leqslant \sqrt[u]{p}$ для фиксированного u.

Для группы точек на эллиптической кривой $E[\mathbb{F}_r]$ над конечным полем $\mathbb{F}_r$ из простого числа элементов r, обозначим $[n]P$ сумму n точек P.

Пусть по двум точкам $Q, P \in E[\mathbb{F}_r]$, связанным равенством

$$Q = [n]P,$$

надо найти n, определённое по модулю $p = \operatorname{ord} P$. Обозначим сложность этой задачи $\mathrm{DLE}(r,p)$, а сложность вычисления $[n_1 n_2]P$ по паре $([n_1]P, [n_2]P)$ — $\mathrm{DHE}(r,p)$. Будем полагать, что эта последняя задача не проще одной операции на эллиптической кривой $E[\mathbb{F}_r]$. Через $\log$ будем обозначать логарифм по некоторому фиксированному основанию, значение которого каждый раз будет некоторой эффективной абсолютной константой.

Теорема 1.

$$\mathrm{DLE}(r,p) \leqslant \mathrm{DHE}(r,p) \log p \sum_{i=1}^{t} {q_i}^{\alpha_i}.$$

Доказательство. Очевидно, что $n \equiv 0 \pmod p$ тогда и только тогда, когда Q является бесконечно удалённой точкой. В противном случае $n \equiv g^h \pmod p$, где g — первообразный корень по модулю p, а h определено по модулю $p-1$. Далее вместо n будем искать h.

Отметим, что множество точек $[n]P$, $n \not\equiv 0 \pmod p$ образует циклическую группу порядка $p-1$ относительно операции

$$[n_1]P * [n_2]P = [n_1 n_2]P,$$

которую будем обозначать G.

Пусть $q \mid p-1$. Будем перебирать случайные $j_0', j_0'' \in \{1, \ldots, (p-1)/q\}$ и проверять, существует ли такое $i \in \{0, 1, \ldots, q-1\}$, что

$$\left[g^{j_0'}\right]Q = \left[g^{j_0''}\right]\left[g^{\frac{p-1}{q}i}\right]P. \tag{2}$$

Если да, то

$$n \equiv g^{j_0'' + p - 1 - j_0' + \frac{p-1}{q}i} \pmod p,$$

или

$$h \equiv j_0'' - j_0' + \frac{p-1}{q} i \pmod{p-1},$$

или

$$h \equiv j_0'' - j_0' \pmod{\frac{p-1}{q}}.$$

Для построения $\left[g^{j_0'}\right]Q$, $\left[g^{j_0''}\right]P$ достаточно $4\log_2 p \leqslant \log p$ операций сложения на эллиптической кривой.

По известной теореме о парадоксе дней рождения [15] среднее число пар (j_0', j_0''), $j_0', j_0'' \in \{1, \ldots, (p-1)/q\}$, которые необходимо проверить, прежде чем будет получен положительный ответ на вопрос о существовании i, равно $\left(\sqrt{\pi(p-1)/q} + O(1)\right)^2$. При этом j_0' и j_0'' пробегают некоторые случайные независимые подмножества в $\{1, \ldots, (p-1)/q\}$ объёма $\sqrt{\pi(p-1)/q}+O(1)$. Отметим, что в этом месте можно заменить случайный перебор на перебор пар $j_0'' = 0$, $j_0' \in \{1, \ldots, (p-1)/q\}$, что увеличит объём рассматриваемых подмножеств, но не изменит числа проверок.

Если теперь вместо q последовательно подставить $\tilde{q}_j$, для которых $\text{НОК}[(p-1)/\tilde{q}_j] = p-1$, и воспользоваться китайской теоремой об остатках, то получим h по модулю $p-1$, т. е. среднее число проверок есть

$$O\Big(\sum_j \pi \frac{p-1}{\tilde{q}_j}\Big),$$

что при $\tilde{q}_j = (p-1)/{q_j}^{\alpha_j}$, $j = 1, \ldots t$, даёт

$$O\Big(\sum_{i=1}^{t} {q_i}^{\alpha_i}\Big). \tag{3}$$

Равенство (2) означает, что

$$Q_{j_0'+p-1-j_0''} = \big[g^{j_0'+p-1-j_0''}\big]Q \in G_{0,\frac{p-1}{q}} = \Big\{\Big[g^{\frac{p-1}{q}i}\Big]P \mid i = 0, 1, \ldots, q-1\Big\}. \tag{4}$$

Вычисление $Q_{j_0'+p-1-j_0''}$ при известных j_0', j_0'' осуществляется квадратичным алгоритмом и требует не более $2\log_2 p$ умножений по модулю p и $2\log_2 p$ сложений точек на эллиптической кривой, что предполагается сложнее (соответствующие формулы требуют пять умножений в поле на одно сложение на эллиптической кривой).

Отметим, что $G_{0,\frac{p-1}{q}}$ — циклическая подгруппа группы G порядка q. Введём операцию $\cdot$ (см. [4]):

$$k \cdot [n]P = \underbrace{[n]P * \ldots * [n]P}_{k} = [n^k]P.$$

Тогда вопрос о принадлежности (4) является вопросом о разрешимости задачи дискретного логарифмирования в циклической группе G. Поскольку группа порядка q в такой группе единственна, то эта принадлежность выполнена тогда и только тогда, когда

$$\underbrace{Q_{j_0'+p-1-j_0''} * \ldots * Q_{j_0'+p-1-j_0''}}_{q} = [1]P = P, \tag{5}$$

что проверяется со сложностью $2\text{DHE}(r,p)\log_2 q$. Теорема доказана. □

В общем случае можно считать, что (см. [4])

$$\text{DLE}(r,p) \leqslant O\Big(s(p)\log^2 p\big(\text{DHE}(r,p)\big)^{s(p)}\Big),$$

где $s(p)$ — длина наибольшей ветви дерева Пратта [14], для которой на сегодняшний день имеется только тривиальная оценка $s(p) \leqslant \log_2 p$ (см. некоторое развитие в [7]).

Доказанная теорема показывает, в частности, что на подгруппах точек простого порядка p на эллиптических кривых, удовлетворяющих стандарту ГОСТ Р34.10-2012, где $p-1$ раскладывается на «маленькие» простые множители, задачи Диффи—Хеллмана и дискретного логарифмирования полиномиально эквивалентны.

2. Вычисление и применение спариваний и их обращений

2.1. Использование спариваний для решения задачи Диффи—Хеллмана

Определение [9]. Пусть G_1, G_2, G_T — циклические группы. Спариванием назовём отображение

$$e\colon G_1 \times G_2 \to G_T.$$

Будем рассматривать билинейные относительно групповых операций невырожденные спаривания.

Пусть f_1, f_2, f_T — единичные элементы групп G_1, G_2, G_T соответственно. Тогда по определению $e(f_1, G_2) = e(G_1, f_2) = f_T$. Рассмотрим случай, когда $|G_1| = |G_2| = |G_T| = p$ — простое число. В этом случае невырожденность спаривания e эквивалентна существованию таких g_1, g_2, g_T из множеств $G_1 \setminus f_1$, $G_2 \setminus f_2$, $G_T \setminus f_T$ соответственно, что $e(g_1, g_2) = g_T$. При этом для любых $h_1 \in G_1$, $h_T \in G_T$ существует $h_2 \in G_2$ и для любых $h_2 \in G_2$, $h_3 \in G_T$ существует $h_1 \in G_1$, такие что $e(h_1, h_2) = h_T$.

Рассмотрим следующие задачи [9]:

$$\begin{aligned}
&\text{FAPI-1:} \quad D_1 \in G_1,\ z \in G_T \to D_2 \in G_2\colon e(D_1, D_2) = z,\\
&\text{FAPI-2:} \quad D_2 \in G_2,\ z \in G_T \to D_1 \in G_1\colon e(D_1, D_2) = z,\\
&\text{GPI-2:} \quad z \in G_T \to D_1 \in G_1,\ D_2 \in G_2\colon e(D_1, D_2) = z.
\end{aligned}$$

Сложности решения этих задач обозначим I_1, I_2, I_T, соответствующие оракулы — O_1, O_2, O_T, а сложность вычисления спаривания обозначим C. Ввиду предполагаемой простоты p и невырожденности спаривания решение FAPI-i единственно. Обозначим через $\mathrm{DH}(G_i)$ сложность решения задачи Диффи—Хеллмана в группе G_i.

Теорема 2 [9, теорема 1].

$$\mathrm{DH}(G_i) \leqslant I_1 + I_2 + 2C, \quad i \in \{1, 2\}. \tag{6}$$

Для дальнейшего будет важен случай, когда G_2 — конечная группа, вообще говоря, не простого порядка, но имеющая универсальную экспоненту, равную p.

Сложность решения задачи FAPI-2 в этом случае (нахождение хотя бы одного решения) будем обозначать $\tilde{I}_2$.

Аналогично доказательству теоремы 2 можно получить следующую оценку. Пусть (P, aP, bP) — элементы G_1, являющиеся входом для задачи Диффи—Хеллмана в группе G_1. Вычислим $z = e(aP, Q) = e(P, aQ)$ для случайного аргумента $Q \in G_2$, такого что $z \neq f_T$. Вычисляем $O_1(P, z) = \tilde{Q}$, такое что $e(P, \tilde{Q}) = e(aP, Q)$. Такое $\tilde{Q}$ существует: например, $\tilde{Q} = aQ$. Вычислим $z' = e(bP, \tilde{Q}) = e(abP, Q)$. Вычисляем $O_2(z', Q) = abP$. Таким образом, имеем следующую оценку на сложность задачи Диффи—Хеллмана в группе G_1:

$$\mathrm{DH}(G_1) \leqslant I_1 + \tilde{I}_2 + 2C, \quad i \in \{1, 2\}.$$

Применяя теорему 1, находим, что

$$\mathrm{DLE}(r, p) \leqslant \log p (I_1 + \tilde{I}_2 + 2C) \sum_{i=1}^{t} q_i^{\alpha_i}.$$

Рассмотрим функцию $f_{s,Q}$ для произвольного целого s как функцию, определённую равенством

$$\mathrm{div}(f_{s,Q}) = s(Q) - (sQ) - (s-1)(\infty). \tag{7}$$

Такая функция существует согласно [16, следствие III.3.5.]. В ряде случаев значение спаривания [11, 12] задаётся формулой

$$f_{s,Q}(D_2) = \prod_{P \in \mathrm{Supp}\, D_2} f_{s,Q}(P)^{v_P(D_2)}.$$

Пусть u — униформизующий параметр в бесконечности, $v_\infty(f)$ — порядок функции f в бесконечности. Обозначим $\mathrm{lc}_\infty(f) = \big(u^{-v_\infty(f)} f\big)(\infty)$. При этом будем обозначать $f^{\mathrm{norm}} = \big(\mathrm{lc}_\infty(f)\big)^{-1} f$. Для получения однозначного определения $f_{s,Q}(D_2)$ заменим f на f^{norm}.

Значения вида $f_{s,Q}(D_2)$ и использующие их спаривания могут быть вычислены при помощи алгоритма Давенпорта [6] и Миллера [13] и его обобщений [5]. Этот алгоритм линеен относительно длины входа, поэтому сложность вычисления, например, спаривания Вейля будет $O(k \log r)$ операций в поле $\mathbb{F}_q$, $q = r^k$, или $O(k^3 \log^3 r)$ битовых операций.

Пусть имеются двоичная запись числа $s = \sigma_{l-1} \ldots \sigma_0$, $\sigma_{l-1} = 1$, и точки $P = (x_1, y_1) \in E(\mathbb{F}_r)[p]$, $Q = (x_2, y_2) \in E(\mathbb{F}_q)$.

Алгоритм Миллера.

1. $T \leftarrow P$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$
2. для $i = l - 2$ до 0
3. $T \leftarrow [2]T$ $(T = (x_3, y_3))$
4. $\lambda \leftarrow$ угловой коэффициент касательной к кривой E в точке T
5. $f_1 \leftarrow f_1^2 (y_2 - \lambda(x_2 - x_3) - y_3)$
6. $f_2 \leftarrow f_2^2 (x_2 + (x_1 + x_3) - \lambda^2)$

7. если $\sigma_i = 1$, то
8. $T \leftarrow T \oplus P$
9. $\lambda \leftarrow$ угловой коэффициент прямой, проходящей через точки T, P
10. $f_1 \leftarrow f_1(y_2 - \lambda(x_2 - x_3) - y_3)$
11. $f_2 \leftarrow f_2(x_2 + (x_1 + x_3) - \lambda^2)$, конец для
12. вывод $f_{s,P}(Q) = f_1/f_2$

Заметим, что λ не зависит от Q. Поэтому при фиксированном P имеем, что $\deg_{x_2} f_1, \deg_{y_2} f_1, \deg_{x_2} f_2, \deg_{y_2} f_2 \leqslant s$ как многочлены. Аналогичное можно доказать и при фиксированном Q. Действительно, применяя формулы удвоения, получим

$$\deg_{y_1} y_3 = 2, \quad \deg_{x_1} y_3 = 3, \quad \deg_{y_1} x_3 = 2, \quad \deg_{x_1} x_3 = 4,$$
$$\deg_{y_3} \lambda = 2, \quad \deg_{x_3} \lambda = 1.$$

Поэтому на i-м шаге алгоритма

$$\deg_{y_1} y_3, \deg_{y_1} x_3 = 2 \leqslant 2^i, \quad \deg_{x_1} y_3 \leqslant \deg_{x_1} x_3 \leqslant 4^i.$$

Все эти степени ограничены величиной 4^i, а из алгоритма Миллера на i-м шаге имеем

$$\deg_{x_1} \frac{f_1}{f_2} \to 2 \deg_{x_1} \frac{f_1}{f_2} + 8 \cdot 4^i, \quad \deg_{y_1} \frac{f_1}{f_2} \to 2 \deg_{y_1} \frac{f_1}{f_2} + 8 \cdot 2^i,$$

откуда по окончании алгоритма получим

$$\deg_{x_1} \frac{f_1}{f_2} \leqslant 2 \cdot 4^{\log_2 s + 1} = 8s^2, \quad \deg_{y_1} \frac{f_1}{f_2} \leqslant 2 \cdot 2^{\log_2 s + 2} = 8s.$$

Пусть $\mathbb{F}_r$ — конечное поле из r элементов, где r простое. Пусть E — эллиптическая кривая, определённая над $\mathbb{F}_r$, и (∞) — бесконечно удалённая точка. $\#E(\mathbb{F}_r)$ обозначает порядок группы $\mathbb{F}_r$-точек кривой $E(\mathbb{F}_r)$, p — большой простой делитель $\#E(\mathbb{F}_r)$, а k — наименьший натуральный, такой что $p \mid r^k - 1$.

Пусть $P \in G_1 = E[p] \cap \operatorname{Ker}(\pi_r - [1])$ и $Q \in G_2 = E[p] \cap \operatorname{Ker}(\pi_r - [r])$. Для каждого целого s пусть $f_{s,Q}$ — рациональная функция на E с дивизором (7).

Пусть $s = r^i \pmod p$ для некоторого целого i. Пусть D — дивизор, эквивалентный $(P) - (\infty)$, носитель которого не пересекается с $\operatorname{Supp}(f_{s,Q})$. Тогда по [20, теорема 1] (редуцированное) обобщённое спаривание Эйта

$$e(P, Q) = f_{s,Q}(D)^{\frac{r^k - 1}{p}}, \quad f_{s,Q}(D) = \prod_{R \in \operatorname{Supp} D} f_{s,Q}(R)^{v_R(D)},$$

является невырожденным билинейным отображением $G_1 \times G_2$ в подгруппу корней p-й степени из единицы мультипликативной группы $\mathbb{F}_{r^k}^*$, если

$$\gamma_p(s^{\operatorname{ord}^p s} - 1) \leqslant \gamma_p(r^k - 1), \tag{8}$$

где $\gamma_p(x)$ — степень вхождения p в x, а ord_p — порядок по модулю p.

Рассмотрим нередуцированное обобщённое спаривание Эйта

$$\tilde{e}(P,Q) = f_{s,Q}(D)$$

как отображение $G_1 \times E(\mathbb{F}_{r^k})$ в $\mathbb{F}_{r^k}^*/(\mathbb{F}_{r^k}^*)^p$. Это отображение корректно определено, так как $\tilde{e}\big([p]P, E(\mathbb{F}_{r^k})\big) \in (\mathbb{F}_{r^k}^*)^p$, т. е. является единицей фактор-группы. $\tilde{e}\big(P,(\infty)\big) = 1$ по определению. Поскольку дивизор вида (7) при любом s является дивизором функции, то это отображение является гомоморфизмом. В случае выполнения условия (8) по [20, теорема 1] этот гомоморфизм также является невырожденным.

Если все возможные s велики, использование спаривания $f_{s,h,Q}(P)$ из [12] может быть эффективным.

По алгоритму Миллера [13] получаем $f_{s,Q}(x,y)$ или $f_{s,(x,y)}(P)$ в виде рациональных функций

$$\frac{f_1(x,y)}{f_2(x,y)}, \quad \deg_x\left(\frac{f_1}{f_2}\right), \deg_y\left(\frac{f_1}{f_2}\right) \leqslant 8s^2.$$

Для фиксированного $P \in G_1$ имеем, что $x,y \in \mathbb{F}_{r^k}$ и $f_1(x,y), f_2(x,y) \in \mathbb{F}_r(x,y)$. Для фиксированного $Q \in G_2$ имеем, что $x,y \in \mathbb{F}_r$ и $f_1(x,y), f_2(x,y) \in \mathbb{F}_{r^k}(x,y)$. Без ограничения общности будем пользоваться оценками $\deg_x f_i(x,y) = O(s^2)$, $\deg_y f_i(x,y) = 1$.

Для решения уравнения $e\big(Q,(x,y)\big) = z$ получим уравнение

$$\left(\frac{f_1(x,y)}{f_2(x,y)}\right)^{\frac{r^k-1}{p}} = z. \tag{9}$$

Пусть

$$\frac{r^k-1}{p} = \alpha_{k-1}r^{k-1} + \ldots + \alpha_0, \quad \alpha_i \in \{0,1,\ldots,r-1\}.$$

Тогда

$$\prod_{i=0}^{k-1}\left(\left(\frac{f_1(x,y)}{f_2(x,y)}\right)^{r^i}\right)^{\alpha_i} = z.$$

Применяя автоморфизм Фробениуса $k-1$ раз, получим систему

$$\prod_{i=0}^{k-1}\left(\left(\frac{f_1(x,y)}{f_2(x,y)}\right)^{r^i}\right)^{\alpha_{i-j \pmod k}} = z^{r^j}, \quad j = 0,1,\ldots,k-1,$$

где $i-j \pmod k$ — наименьший положительный вычет по модулю k. Рассмотрим

$$\left(\frac{f_1(x,y)}{z f_2(x,y)}\right)^{r^i}, \quad i = 0,\ldots,k-1,$$

как новые мультипликативные переменные. Степени этих переменных образуют циркулянтную матрицу C из $\mathbb{Z}_{r^k-1}^{k\times k}$. Мы хотим получить вектор $\bar{v} \in \mathbb{Z}_{r^k-1}^k$, для

которого $\bar{v}C = (a_1, \ldots, a_k)$, $a_i \in \mathbb{Z}$, где

$$\sum_{i=1}^{k} |a_i| \leqslant |\bar{a}| = a$$

с малым $a \in \mathbb{N}$.

С помощью алгоритма Ленстры—Ленстры—Ловаса [17, теорема 7.11] можно получить вектор $(a_1, \ldots, a_k)$ как наименьший вектор в решётке строк матрицы C за $O(k^4 \log r)$ арифметических операций с небольшими целыми (модуль которых меньше $O(k \log r)$). Согласно [17, теорема 7.7] получим [10]

$$a \leqslant 2^{\frac{k-1}{4}} (\det C)^{\frac{1}{k}}, \quad \det C = \prod_{j=0}^{k-1} \sum_{t=0}^{k-1} \alpha_i e^{\frac{2\pi i}{k} jt}.$$

Похожие рассуждения в [18] приводят к той же целочисленной решётке. Для выяснения возможности нахождения малого вектора a в циклотомической решётке, описанной выше, был поставлен численный эксперимент.

В результате эксперимента с пятизначными простыми малых векторов найти не удалось (координаты минимального вектора в основном пятизначные). Ситуация существенно не улучшилась при добавлении в рассматриваемую решётку векторов показателей, которые дают корни из единицы не очень большой степени, которые можно было бы потом перебрать.

Для решения поставленной задачи воспользуемся нередуцированным обобщённым спариванием Эйта в случае, когда оно невырожденно. Значения этого спаривания лежат в фактор-группе $\mathbb{F}_{r^k}^*/(\mathbb{F}_{r^k}^*)^p$. Таким образом, обращение такого спаривания может быть сведено к решению уравнения

$$\frac{f_1(x,y)}{f_2(x,y)} = z(\tilde{z})^p, \quad \tilde{z} \in \mathbb{F}_{r^k}^*. \tag{10}$$

Для уменьшения степени в правой части этого уравнения рассмотрим преобразование $i\colon r^i \equiv s \pmod p$. Предположим, что s мало и выполнено условие (8). Пусть, кроме того, $t = (r^i - s)/p$, $(t, (r^k - 1)/p) = 1$. Если это условие не выполняется, нужно рассмотреть удовлетворяющее этому условию $t = \big(\sum \alpha_i r^i\big)/p \in \mathbb{Z}$ с маленькими целыми значениями α_i (по модулю меньшими, чем s^2). Если считать вычеты $\sum \alpha_i r^i \pmod p$, а также $\big(\sum \alpha_i r^i\big)/p \,(\mathrm{mod}\ ()r^k - 1)/p$ при $\big(\sum \alpha_i r^i\big)/p \in \mathbb{Z}$ случайными, то с хорошей вероятностью это произойдёт при $(2s^2)^k > 2p \ln\ln\big((r^k - 1)/p\big)$, или при

$$s^k > p. \tag{11}$$

Вместо уравнения (10) будем рассматривать аналогичное

$$\frac{f_1(x,y)}{f_2(x,y)} = z(\tilde{z})^{pt}, \quad \tilde{z} \in \mathbb{F}_{r^k}^*.$$

Поскольку $pt \equiv r^i - s \pmod r)^k - 1$, получим

$$\frac{f_1(x,y)}{f_2(x,y)} = z(\tilde{z})^{r^i - s}. \tag{12}$$

В случае фиксированного Q имеем $x, y \in \mathbb{F}_r$ и

$$\deg\left(\frac{f_1(x,y)}{f_2(x,y)}\right) = O(s^2).$$

Элемент $\tilde{z} \in \mathbb{F}_{r^k}$ может быть представлен в нормальном базисе [1]:

$$\tilde{z} = z_1\theta^{r^0} + z_2\theta^{r^1} + \ldots, \quad z_k\theta^{r^{k-1}},\ z_i \in \mathbb{F}_r,$$
$$\tilde{z}^{r^i} = z_{1-i \pmod k}\theta^{r^0} + \ldots, \quad z_{k-i \pmod k}\theta^{r^{k-1}}.$$

Произведение таких элементов может быть записано в той же форме с коэффициентами, являющимися квадратичными формами от исходных коэффициентов. Умножая на знаменатель, получим

$$\Phi(x, y, z_1, \ldots, z_k) = 0, \quad \Phi \in \mathbb{F}_{r^k}[x, y], \quad \deg\Phi = O(s^2).$$

В случае $\#E(\mathbb{F}_r) = p$ любое решение системы, состоящей из этого уравнения и уравнения кривой, даёт точку, принадлежащую $\langle P\rangle$.

В случае фиксированного P в (12) получим $x, y \in \mathbb{F}_{r^k}$, которые, как и выше, могут быть представлены в нормальном базисе:

$$x = x_1\theta^{r^0} + x_2\theta^{r^1} + \ldots, \quad x_k\theta^{r^{k-1}},\ x_i \in \mathbb{F}_r,$$
$$y = y_1\theta^{r^0} + y_2\theta^{r^1} + \ldots, \quad y_k\theta^{r^{k-1}},\ y_i \in \mathbb{F}_r.$$

Таким образом, в обоих случаях, представив z, $\tilde{z}$ и коэффициенты многочленов из $\mathbb{F}_{r^k}$ в нормальном базисе и собрав коэффициенты при θ^{r^i} за $O(s^2k^2)$ арифметических операций в $\mathbb{F}_r$, можно представить уравнение (12) как систему из k уравнений степени $O(s^2)$ над $\mathbb{F}_r$ от $x, y, z_1, \ldots, z_k$ или $x_1, \ldots, x_k$; $y_1, \ldots, y_k$; $z_1, \ldots, z_k$, лежащих в $\mathbb{F}_r$. Уравнение кривой $y^2 = x^3 + \alpha x + \beta$ даст ещё одно или k уравнений над $\mathbb{F}_r$ соответственно. Общая система из этих уравнений может быть решена методами, использующими базис Грёбнера, или другими методами решения полиномиальных систем, когда s, k невелики. Оценка сложности применения в этом случае (переменных больше, чем уравнений) алгоритма F_5 [8] следующая:

$$O(k(s^2)^{3\cdot 3k}). \tag{13}$$

Она, очевидно, является оценкой сложности всего алгоритма обращения спаривания.

Важно напомнить, что, как было замечено в [19], поскольку p простое, то из того, что $d = \operatorname{ord}_p s$, $s \equiv r^i \pmod p$, следует, что p делит значение кругового многочлена $Q_d(s)$. Тогда $s \geqslant p^{\frac{1}{d}} \geqslant p^{\frac{1}{k}}$. При этом условие (11) выполняется, но при подстановке в (13) оценка сложности получается слишком большой. Однако, если рассматриваемая система полиномиальных уравнений не является полурегулярной (см., например, [2]), например как в случае HFE, она решается теми же алгоритмами намного быстрее.

В систему полиномиальных уравнений, которую мы предлагаем решать, можно включать уравнения, полученные из уравнений вида

$$\tilde{e}([m]P, Q) = z^m(\tilde{z}_1)^p, \quad \tilde{e}(P, [m]Q) = z^m(\tilde{z}_2)^p, \quad \tilde{z}_i \in \mathbb{F}^*_{r^k}.$$

Также отметим, что вместо нормального базиса можно использовать любой другой. Автоморфизм Фробениуса действует в этом базисе как некоторый линейный оператор.

Литература

[1] Ван дер Варден Б. Л. Алгебра. — М.: Наука, 1976.

[2] Bardet M., Faugère J. C., Salvy B. Complexity of Gröbner basis computation for semi-regular overdetermined sequences over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$: INRIA, Rapport de Recherche No. 5049, Decembre 2003.

[3] Canfield E. R., Erdős P., Pomerance C. On a problem of Oppenheim concerning "Factorisatio Numerorum" // J. Number Theory. — 1983. — Vol. 17. — P. 1—28.

[4] Cherepnev M. A. On the connection between discrete logarithms and the Diffie—Hellman problem // Discrete Math. — 1996. — Vol. 8, no. 3. — P. 22—30.

[5] Cohen H., Frey G., et al. Handbook of Elliptic and Hyperelliptic Curve Cryptography. — London: Chapman and Hall, 2006.

[6] Davenport J. H. On the Integration of Algebraic Functions. — Berlin: Springer, 1979. — (Lect. Notes Comput. Sci.; Vol. 102).

[7] Ford K., Konyagin S. V., Luca F. Prime chains and Pratt trees // Geom. Funct. Anal. — 2010. — Vol. 20. — P. 1231—1258.

[8] Faugère J. C., Din M. S., Verron T. On the complexity of computing Gröbner basis for quasi-homogeneous systems // ISSAC'13. June 26-29, 2013, Boston, Massachusetts, USA.

[9] Galbraith S., Hess F., Vercauteren F. Aspects of pairing invertion // IEEE Trans. — 2008. — Vol. 54, no. 12. — P. 5719—5728.

[10] Gradshteyn I. S., Ryzhik I. M. Tables of Integrals, Series, and Products. — San Diego: Academic Press, 2000. — P. 1111—1112.

[11] Hess F. A note on the Tate pairing of curves over finite fields // Arch. Math. (Basel). — 2004. — Vol. 82. — P. 28—32.

[12] Hess F. Pairing Lattices // Pairing Based Cryptography — Pairing 2008 / S. D. Galbraith, K. G. Paterson, eds. — Berlin: Springer, 2008. — (Lect. Notes Comput. Sci.; Vol. 5209). — P. 18—38.

[13] Miller V. S. Short Programs for Functions on Curves: Unpublished manuscript. — 1986. — `http://crypto.stanford.edu/miller/`.

[14] Pratt V. Every prime has a succinct certificate // SIAM J. Comput. — 1975. — Vol. 4, no. 3. — P. 214—220.

[15] Selivanov B. I. On waiting time in the scheme random allocation of coloured particles // Discrete Math. Appl. — 1995. — Vol. 5, no. 1. — P. 73—82.

[16] Silverman J. The Arithmetic of Elliptic Curves. — Berlin: Springer, 1986.

[17] Vasilenko O. N. Number-Theoretic Algorithms in Cryptography. — 2006.

[18] Vercauteren F. The hidden root problem // Pairing Based Cryptography — Pairing 2008 / S. D. Galbraith, K. G. Paterson, eds. — Heidelberg: Springer, 2008. — (Lect. Notes Comput. Sci.; Vol. 5209). — P. 89—99. — `https://eprint.iacr.org/2008/261.pdf`.

[19] Vercauteren F. Optimal Pairings // IEEE Trans. Inform. Theory. — 2010. — Vol. 56, no. 1. — P. 455—461. — https://eprint.iacr.org/2008/096.pdf.

[20] Zhao C.-A., Zhang F., Huang J. A note on the Ate pairing cryptology. — http://eprint.iacr.org/2007/247.pdf.