УДК 004.056.53
М.А.Черепнёв, д-р физ. мат. наук, с.н.с., e-mail: cherepniov@gmail.com,
АО "Концерн "Автоматика"
С.С.Грачева канд. тех. наук, доц., e-mail: statgracheva@mail.ru,
Национальный исследовательский университет "Высшая школа экономики"

Решение задачи Диффи-Хеллмэна на некоторых эллиптических кривых, удовлетворяющих ГОСТ 34.10-2018.

Аннотация

Сатья посвящена криптоанализу часто используемой схемы Диффи-Хеллмэна открытого распределения ключа. Начиная со статьи [1], идея которой ранее была изложена в работах И.Семаева, значительный интерес с точки зрения атакующих криптопротоколы на эллиптических кривых, стала преобретать степень расширения или MOV-степень. В англоязычной литературе этот параметр (далее k) принято называть "embedding degree". Имеется ввиду расширение поля коэффициентов эллиптической кривой, в котором содержатся все точки исходного простого порядка p. Случайное значение этого параметра приближается к значению p, что приводит к длине записи элемента соответствующего расширения не многим меньше чем $p \log p$. В стандарте ГОСТ 34.10-2018 этот параметр предлагается брать больше 31, что позволяет использовать данное расширение, поскольку длина записи его элементов не больше $k \log p$. В данной статье предложен полиномиальный алгоритм решения распознавательной и обычной задачи Диффи-Хеллмэна, эффективный для некоторых таких кривых. Это означает, что схемы открытого распределения ключа, построенные с использованием этих кривых являются нестойкими. Предлагаемый алгоритм основан на выборе такого спаривания, которое нетривиально определено на всех точках порядка p и может быть представлено в виде рациональной функции относительно небольшой степени. Сведение задачи Диффи-Хеллмэна к такому обращению получено в работе [2]. За основу предлагаемой конструкции взято нередуцированное спаривание Эйта, использованное в работе [19]. Предложены новые механизмы для расширения области определения рассматриваемого спаривания с помощью автоморфизма Фробениуса и сведения обращения по второму аргументу (лежащему в расширении поля коэффициентов кривой) к решению системы линейных уравнений с последующим поиском корней многочленов небольшой степени. Представлены оценки на вероятность разрешимости получаемых уравнений при взятии случайного представителя смежного класса, представляющего значение спаривания.

Ключевые слова: схема открытого распределения ключа, эллиптические кривые, задача Диффи-Хеллмэна, спаривание Тэйта, спаривание Эйта, автоморфизм Фробениуса.

Введение

Для построения современных схем защиты информации довольно часто используют группу точек на эллиптической кривой. Составной частью многих схем шифрования является протокол открытого распределения ключа Диффи-Хеллмэна. В данной работе получены условия на размер основного поля и порядок используемой группы точек существующей эллиптической кривой, достаточные для решения на ней задачи Диффи-Хеллмэна с полиномиальной сложностью. Отметим, что при псевдослучайном характере построения эллиптических кривых, вероятность, с которой выполняются указанные условия, пренебрежимо мала. С другой

стороны, некоторые кривые с малой MOV-степенью построены в [8], хотя в общем случае задача построения таких кривых пока не решена.

Полиномииальные алгоритмы, решающие ту же задачу для некоторых суперсингулярных кривых со стенью расширения равной 2 или 3 предложены в работе [3]. Быстрые алгоритмы обращения алгоритма Миллера предложены для некоторых кривых в работах [4, 5, 6, 7] в случаях, когда степень расширения не превосходит 12, либо [11] для случая, когда имеется невырожденное спаривание, выражающееся рациональной функцией малой степени с однозначно определенными значениями в конечном поле (без доказательства его существования). В данной работе предложен полиномиальный алгоритм решения задачи Диффи-Хеллмэна, включающий построение невырожденного спаривания, выражающегося рациональной функцией малой степени (при выполнении некоторых необременительных требований на параметры кривой), со значениями в факторгруппе конечного поля (спаривание Эйта) и обращение алгоритма Миллера для такого спаривания для некоторых кривых с полиномиальной границей на степень расширения.

Рассмотрим эллиптическую кривую над большим простым полем $\mathbb{F}_r$ из r элементов

$$y^2 = x^3 + ax + b, a, b \in \mathbb{F}_r.$$

Для некоторого простого, отличного от r, делителя p порядка группы $E(\mathbb{F}_r)$, состоящей из $\mathbb{F}_r$ точек этой кривой, рассмотрим все точки порядка p, координаты которых лежат в алгебраическом замыкании $\overline{\mathbb{F}}_r$. Пусть $k = ord_p r > 1$, а ord_p — порядок по модулю p. Хорошо известно [9, 16], что все эти точки образуют группу, являющуюся прямым произведением двух групп порядка p.

$$E[p] = G_1 \times G_2,$$

где $G_1 = E[p] \cap Ker(\pi_r - [1]), G_2 = E[p] \cap Ker(\pi_r - [r]) \in E(\mathbb{F}_{r^k})$,

Пусть $e(G_1, G_2)$ - невырожденное билинейное спаривание, то есть гомоморфизм, отличный от тождественной единицы. Аналогично тому, как это было сделано в [10, 11] можно получить следующую оценку сложности решения распознавательной задачи Диффи-Хеллмэна. Пусть (P, aP, bP, P') — элементы G_1, являющиеся входом для распознавательной задачи Диффи-Хеллмэна в группе G_1. Пусть $e(P, Q)$ для некоторого случайного аргумента $Q \in G_2$ отлично от единицы. Вычислим $\tilde{Q}$ такое, что $e(P, Q)^b = e(bP, Q) = e(P, \tilde{Q})$. Такое $\tilde{Q}$ существует, например $\tilde{Q} = bQ$. Проверим $e(aP, \tilde{Q}) = e(P, \tilde{Q})^a = e(P', Q)$. Если да, то $P' = abP$. Таким образом, имеем следующую оценку на сложность распознавательной задачи Диффи-Хеллмэна в группе G_1:

$$DDH(G_1) \leq I_2 + 3C,$$

где C - сложность вычисления спаривания, а I_2 - сложность обращения спаривания по второму аргументу. Аналогично

$$DDH(G_2) \leq I_1 + 3C,$$

а для сложности решения обычной задачи Диффи-Хеллмэна

$$DH(G_i) \leq I_1 + I_2 + 2C, i \in \{1, 2\}.$$

Рассмотрим рациональную функцию $f_{s,Q}(x, y)$ для произвольного целого s как функцию, определённую равенством

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

Такая функция существует согласно [9, Следствие III.3.5.]. В ряде случаев значение спаривания [16, 17] задаётся формулой

$$f_{s,Q}(D_2) = \prod_{P \in SuppD_2} f_{s,Q}(P)^{v_P(D_2)}. \quad (2)$$

Значения вида $f_{s,Q}(D_2)$ и использующие их спаривания могут быть вычислены при помощи алгоритма Давенпорта [12] - Миллера [13] и его обобщений [15]. Этот алгоритм линеен относительно длины входа, поэтому сложность вычисления, например, спаривания Вейля будет $O(klogr)$ операций в поле $\mathbb{F}_{r^k}$, или $O(k^3log^3r)$ битовых операций.

Спаривание Эйта [18] выражается формулой (2) с одним множителем. Пусть $P \in G_1$, и $Q \in G_2$.

Пусть

$$s = r^i(modp), 1 \leq i \leq k-1. \quad (3)$$

Тогда [19][Theorem 1] обобщённое спаривание Эйта

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

является невырожденным билинейным отображением $G_1 \times G_2$, если

$$\gamma_p(s^{ord_p s} - 1) \leq \gamma_p(r^k - 1), \quad (4)$$

где $\gamma_p(x)$ — степень вхождения p в x.

1. Представление элементов смежных классов

Для простоты дальнейших рассуждений будем считать, что $p^2 \nmid r^k - 1$. Это, в частности, означает, что в $\mathbb{F}^*_{r^k}$ нет подгруппы порядка p^2, подгруппа порядка p единственна, а также в каждом смежном классе факторгруппы $\mathbb{F}^*_{r^k} / (\mathbb{F}^*_{r^k})^p$, существует единственный элемент порядка p. Рассмотрим этот вопрос несколько подробнее. Представим абелеву группу $\mathbb{F}^*_{r^k}$ в виде разложения на примарные группы, соответствующие различным простым делителям числа $r^k - 1 = \prod_{i=1}^{i_0} p_i^{\alpha_i}$:

$$\mathbb{F}^*_{r^k} = \bigotimes_{i=1}^{i_0} < g_i >_{p_i^{\alpha_i}}, p_1 = p, \alpha_1 = 1,$$

тогда

$$(\mathbb{F}^*_{r^k})^p = \bigotimes_{i=1}^{i_0} < g_i^p >_{p_i^{\alpha_i}} = \bigotimes_{i=2}^{i_0} < g_i >_{p_i^{\alpha_i}},$$

так как $g_1^p = 1, ordg_i^p = {p_i}^{\alpha_i}$ при $i > 1$. Таким образом факторгруппа $\mathbb{F}^*_{r^k} / (\mathbb{F}^*_{r^k})^p$ изоморфна циклической группе $< g_1 >_p$ порядка p. Смежные классы этой факторгруппы состоят из элементов

$$g_1^{\beta_1} \prod_{i=2}^{i_0} g_i^{\beta_i}, \beta_i = 0, 1, \ldots, {p_i}^{\alpha_i} - 1,$$

при фиксированном $\beta_1 \in \{0, 1, \ldots, p-1\}$.

Определение 1 *Элеманты вида*

$$\prod_{i=2}^{i_0} g_i^{\beta_i}, \beta_i = 0, 1, \ldots, p_i^{\alpha_i} - 1,$$

перечисляющие смежный класс, в соответствующей факторгруппе, будем называть сдвигом

Аналогично, для произвольного натурального n,

$$(\mathbb{F}_{r^k}^*)^n = \bigotimes_{i=1}^{i_0} < g_i^{p_i^{\gamma_i}} >_{p_i^{\alpha_i - \gamma_i}},$$

где $p_i^{\gamma_i} = (n, p_i^{\alpha_i})$. Таким образом факторгруппа $\mathbb{F}_{r^k}^* \diagup (\mathbb{F}_{r^k}^*)^n$ состоит из смежных классов

$$\prod_{i=1}^{i_0} {g_i}^{\delta_i} {g_i}^{p_i^{\gamma_i} \beta_i},$$

при фиксированных $\delta_i = 0, 1, \ldots, p_i^{\gamma_i} - 1$, и произвольных $\beta_i \in \{0, 1, \ldots, p_i^{\alpha_i - \gamma_i} - 1\}$.

При этом она изоморфна циклической группе

$$\bigotimes_{i=1}^{i_0} < g_i^{p_i^{\alpha_i - \gamma_i}} >_{p_i^{\gamma_i}} .$$

Соответственно свиг имеет вид

$$\prod_{i=1}^{i_0} {g_i}^{p_i{}^{\gamma_i} \beta_i}, \beta_i = 0, 1, \ldots, p_i^{\alpha_i - \gamma_i} - 1.$$

А мощность сдвига равна

$$\sharp(\mathbb{F}_{r^k}^*)^n = \prod_{i=1}^{i_0} p_i^{\alpha_i - \gamma_i} = \frac{r^k - 1}{(n, r^k - 1)}.$$

Все решения уравнения $X^n = 1$ в $\mathbb{F}_{r^k}^*$ будут иметь вид

$$\prod_{i=1}^{i_0} {g_i}^{p_i^{\alpha_i - \gamma_i} \beta_i}, \beta_i \in \{0, 1, \ldots, p_i^{\gamma_i} - 1\},$$

а состоящая из них группа изоморфна факторгруппе $\mathbb{F}_{r^k}^* \diagup (\mathbb{F}_{r^k}^*)^n$.

Циклической структурой мультипликативной группы поля $\mathbb{F}_{r^k}^*$ мы здесь (после определения 1) не пользовались, то есть p_i не обязательно различны. Так что теже выкладки можно провести для аддитивной группы точек на эллиптической кривой и её факторгруппы по n кратным точкам, которая будет изоморфна подгруппе $\ker[n]$.

2. Модельный пример

Из билинейности следует, что образом для различных видов спариваний, определённых на $G_1 \times G_2$, является некоторая группа порядка p, образованная элементами $\mathbb{F}_{r^k}$. Предположим сначала, что для спаривания Эйта на некоторой эллиптической кривой эта группа является

единственной подгруппой $G \subset \mathbb{F}_{r^k}^*$ порядка p. То есть все элементы образа этого спаривания лежат в $< g_1 >_p$. Это модельный пример. Здесь мы не будем обсуждать бывает такое или нет

Из формулы (5) на стр. 239 [14] (см. также алгоритм Миллера [13, 15]) при $s = 2$ получаем

$$f_{2,Q}(P) = \frac{y_1 - \lambda(x_1 - x_2) - y_2}{x_1 - x_3},$$

где $P(x_1, y_1), Q(x_2, y_2), [2]Q(x_3, y_3), \lambda = \frac{3x_2^2+a}{2y_2}$. Поэтому, обращение рассматриваемого спаривания по первому аргументу, то есть по P — это решение системы

$$\begin{cases} \frac{y_1-\lambda(x_1-x_2)-y_2}{x_1-x_3} = z \\ y_1^2 = x_1^3 + ax_1 + b \end{cases} \tag{5}$$

относительно $x_1, y_1 \in \mathbb{F}_r$ при фиксированных $x_2, y_2, x_3, y_3, \lambda \in \mathbb{F}_{r^k}; a, b \in \mathbb{F}_r, z \in G$.

Исключая y_1 из первого уравнения, получим кубическое уравнение на x_1. Решая его (это можно сделать по формулам Кардано за $O(1)$ операций в $\mathbb{F}_{r^k}$), получим не более шести точек в $E(\mathbb{F}_r)$, которые можно проверить на принадлежность к G_1, проверяя $[p]P = \infty$, не более чем за $O(\log p)$ операций в $\mathbb{F}_r$. Поскольку исходное уравнение заведомо имело решение в G_1, то мы его получим. Можно поступить и иначе, заменив в системе (5) координаты точек $Q, [2]Q$ соответственно на координаты точек $[t]Q, [2t]Q$, а z на z^t для некоторого небольшого t. Тогда получим ещё одно кубическое уравнение на x_1. Искомая точка $P \in G_1$ будет, очевидно, решением обоих уравнений. Естественно предположить, что эти уравнения будут разными, поэтому, исключая x_1^3 из двух кубических уравнений, получим квадратное уравнение на x_1. Выбрав ещё одно значение для t, получим x_1.

Действуя аналогичным образом в случае небольшого $s > 2$, или в случае обращения спаривания по второму аргументу, сначала подстановкой второго уравнения исключаем из первого уравнения системы вида (5), с переменными соответственно $x' = x_1, y' = y_1$ или $x' = x_2, y' = y_2$, все степени переменной y', большие единицы. Затем в получившемся уравнении выражаем y' через x' и подставляем во второе уравнение. Получится полином от x' степени $O(s)$ (см. формулу (5) на стр. 239 [14]), среди корней которого, как и раньше найдём координату искомой точки. При этом, в случае обращения по второму аргументу при отборе корней нужна дополнительная проверка $\pi_r(Q) = [r]Q$.

Вместо проверки $[p]P = \infty$ можно предложить процедуру побыстрее (схожие идеи описаны в [21]). Если $E(\mathbb{F}_r) = G_1 \times \tilde{G}$ для некоторой группы $\tilde{G}$ с небольшим порядком t, что обычно бывает в криптографически значимых случаях, то для получения искомой точки $P \in G_1$ надо для произвольного решения $\tilde{P} \in E(\mathbb{F}_r)$ воспользоваться тем, что $(p, t) = 1$, откуда $P = [1 + kp]\tilde{P}$ для k, удовлетворяющего $1 + kp \equiv 0 \pmod{t}$.

3. Свойства спаривания Тэйта

Рассмотрим теперь N спаривание Тейта $f_{N,Q}(P)$ [17] для некоторого натурального N. Гомоморфным образом рассматриваемого спаривания на $(P, Q) \in E(\mathbb{F}_{r^k})[N] \times E(\mathbb{F}_{r^k}) / [N]E(\mathbb{F}_{r^k})$ является факторгруппа $G = \mathbb{F}_{r^k}^* / (\mathbb{F}_{r^k}^*)^N$. Следует иметь ввиду, что, как было показано ранее, имеется изоморфизм $E(\mathbb{F}_{r^k})[N] \cong E(\mathbb{F}_{r^k}) / [N]E(\mathbb{F}_{r^k})$.

Теорема 1 *(Теорема 3 [17]) Спаривание $f_{N,Q}(P)$ является билинейным и невырожденным, если поле $\mathbb{F}_{r^k}$ содержит корень N-ой степени из единицы.*

Причем невырожденность в этой теореме понимается в «особом» смысле. То есть спаривание $t : A \times B \to Z$ на абелевых группах A, B, Z невырождено в «особом» смысле, если соответствующие гомоморфизмы $A \to Hom(B; Z)$ и $B \to Hom(A; Z)$ инъективны.

Свойство гомоморфизма переводить сумму точек в произведение их образов будем в дальнейшем называть линейностью. Поскольку при этом порядок точек образа делит порядок точек прообразов (в данном случае их два), то значение спаривания в указанной факторгруппе зависит только от примарных компонент области определения, для которых соответствующие простые входят в НОД($\sharp E(\mathbb{F}_{r^k})[N], r^k - 1$).

Наличие в $\mathbb{F}_{r^k}$ корня из единицы степени N или циклической группы порядка N, означает, что $N = \prod_{i=0}^{i_0} p_i^{\gamma_i}$ делит $r^k - 1 = \prod_{i=0}^{i_1} p_i^{\alpha_i}$, то есть $\alpha_i \geq \gamma_i, i = 0, 1, \ldots, i_0, i_1 \geq i_0$ (здесь все p_i различны). Для некоторого $p = p_i, i \leq i_0$ пусть g и $\overline{g}$ образующие соответствующих примарных компонент порядка p^δ в разложении изоморфных групп $E(\mathbb{F}_{r^k})[N] \cong E(\mathbb{F}_{r^k}) \diagup [N]E(\mathbb{F}_{r^k})$. Пусть $f_{N,\overline{g}}(g) = \tilde{g} \in \mathbb{F}^*_{r^k}/(\mathbb{F}^*_{r^k})^N$. Тогда из линейности получаем, что $ord\tilde{g} = p^\sigma, \delta \geq \sigma$ (так как единица переходит в единицу), а $\sigma \leq \alpha_i - \gamma_i$. Далее $f_{N,\overline{g}^a}(g^b) = \overline{\tilde{g}}^{Cab}$, для некоторой константы C, где $ord\overline{\tilde{g}} = p_i^{\alpha_i - \gamma_i}$. Если группа $E(\mathbb{F}_{r^k})[N]$ содержит несколько примарных компонент, отвечающих одному простому p, то значение спаривания на них будет иметь вид

$$\overline{\tilde{g}}^{C_1 a_1 b_1 + \cdots + C_j a_j b_j}. \tag{6}$$

Причем из линейности это значение не зависит от примарных компонент аргументов рассматриваемого спаривания, отвечающих простым не равным p. Элементы примарных компонент аргументов, для которых соответствующие простые p не содержатся среди p_i могут влиять лишь на сдвиг (предположительно случайно). Таким образом доказана следующая

Теорема 2 *Пусть $\mathbb{F}^*_{r^k}/(\mathbb{F}^*_{r^k})^N = \prod_i \tilde{G}_i$ — разложение в примарные компоненты $\sharp\tilde{G}_i = {p_i}^{\alpha_i}$. Рассмотрим i-ю координатную функцию рассматриваемого спаривания, отвечающую компоненте $\tilde{G}_i$, где соответствующее p_i делит $\sharp E(\mathbb{F}_{r^k})$. Тогда в условиях теоремы 1 она линейно, невырожденно и корректно отображает произведения элементов примарных компонент области определения, отвечающих одному и тому же простому p_i на примарную группу $\tilde{G}_i$. Примарные компоненты области определения, соответствующие простым, не входящим в НОД($\sharp E(\mathbb{F}_{r^k})[N], r^k - 1$) влияют только на сдвиг (то есть меняют представителя но не класс смежности в который попадает результат спаривания).*

Корректность означает независимость от примарных компонент, отвечающих другим простым. Из теоремы 2, в частности следует, что координатные функции, отвечающие простым, не входящим в НОД($\sharp E(\mathbb{F}_{r^k})[N], r^k - 1$) тождественно равны единице. Следует также иметь ввиду, что количество примарных компонент в группе точек на эллиптической кривой, отвечающих одному простому числу ограничено двумя (следствие 6.4 стр.89 [9]). Поэтому количество слагаемых в показателе равенства (6) не более четырёх.

Заметим, что выполнения условия существования соответствующего корня из единицы можно добиться перейдя к расширению поля $\mathbb{F}_{r^k}$, а именно, добавив все корни многочлена $X^N - 1$, то есть $\mathbb{F}_{r^{kw}}$, где $w = ord_N r^k$. При этом, если $E(\mathbb{F}_{r^k}) \in [N]E(\mathbb{F}_{r^{kw}})$, то на аргументах из $E(\mathbb{F}_{r^k})$ рассматриваемое спаривание принимает только значение в единичном смежном классе. Однако, если в качестве N взять универсальную экспоненту группы $E(\mathbb{F}_{r^k})$, условие $E(\mathbb{F}_{r^k}) \in [N]E(\mathbb{F}_{r^{kw}})$ приводит к необходимости того, чтобы универсальная экспонента группы $E(\mathbb{F}_{r^{kw}})$ делилась на N^2. Из-за аддитивной зависимости между порядками эллиптической кривой над полем и его расширением, проследить при каких r, k это бывает в общем виде достаточно трудно.

Для построения спаривания Тейта, определенного на всех точках $E(\mathbb{F}_{r^k})$, необходимо выбирать в качестве N кратное универсальной экспоненте группы $E(\mathbb{F}_{r^k})$. Но наличие дополнительных множителей может привести к вырождению, то есть к увеличению объёма сдвига, чего нам бы не хотелось. Проведя численные эксперименты, мы в ряде случаев убедились, что при выборе в качестве N универсальной экспоненты группы $E(\mathbb{F}_{r^k})$ спаривание Тейта не тождественно равно единице на $E(\mathbb{F}_{r^k})\times E(\mathbb{F}_{r^k})$. Однако оно выражается рациональной функцией слишком большой степени, что не позволяет быстро его обращать.

4. Вариант спаривания с сжимающими отображениями

Пусть x - какой либо корень характеристического многочлена автоморфизма Фробениуса π_r по модулю N:

$$x^2 - tx + r \equiv 0(modN), t = r + 1 - \sharp(E(\mathbb{F}_r)), x \equiv r \pmod p. \tag{7}$$

(В этом месте можно использовать также характеристическое уравнение для $\pi_{r^l} : x^2 - t_l x + r^l \equiv 0 \pmod N, t_l = 1 + r^l - \sharp(E(\mathbb{F}_{r^l}))$. Тогда, очевидно, $(x, N) = 1$, при $r \nmid N$. Поскольку $t_l = \alpha^l + \beta^l$, где $\alpha\beta = r, \alpha + \beta = t$ (Теорема 2.4 [9]), то $t_k \equiv t^k \pmod r$, так как симметрический многочлен от α, β с целыми коэффициентами является целым числом. Подставляя t^k в выражение для t_k получим $t^k \equiv 1 - \sharp(E(\mathbb{F}_{r^k})) \pmod r$, откуда, ввиду того, что N и $\sharp(E(\mathbb{F}_{r^k}))$ состоят из одинаковых простых множителей, получим, что условие $r \nmid N$ равносильно тому, что $ord_r t \nmid k$. Это и будем в дальнейшем предполагать

Поскольку $x - t + rx^{-1} \equiv 0(modN)$, то для любой точки $Q \in E(\mathbb{F}_{r^k})$ и преобразования $\tilde{Q}(Q) = (\pi_r - [rx^{-1}])[n^{-1} \pmod p][n]Q$ имеем $\pi_r\tilde{Q} = (\pi_r^2 - [rx^{-1}]\pi_r)\hat{Q} = ([t - rx^{-1}]\pi_r - [r])\hat{Q} = ([x]\pi_r - [r])\hat{Q} = [x]\tilde{Q}$.

Пусть теперь $T \equiv x^j \neq 1 \pmod N$ мало при некотором j, и $\hat{t} \equiv rx^{-1} \pmod N$. Тогда, в силу (7), $\hat{t} \equiv 1 \pmod p$. Следуя плану, изложенному в [18], построим некоторое новое спаривание. Рассмотрим отображение на $E(\mathbb{F}_{r^k})^2$, заданное равенством

$$\tilde{e}_T(Q, P) = \frac{f'_{T,\tilde{Q}}(trP)}{f'_{T,\tilde{Q}}(\infty)}, \quad \text{где} \quad trP = \sum_{i=0}^{k-1} \pi_r^i P \in E(\mathbb{F}_r), \tilde{Q} = \tilde{Q}(Q + R) \tag{8}$$

где $f'_{T,\tilde{Q}} = \frac{f_{T,\tilde{Q}}}{f_{T,\tilde{R}}}$ для некоторой случайной фиксированной точки $\tilde{R} \in E(\mathbb{F}_{r^k}) \bigcap Ker(\pi_r - [x])$, например $\tilde{R} = \tilde{Q}(R), R \in E(\mathbb{F}_{r^k})$.

Для редуцированного N спаривания Тэйта имеем (см. [17] определение 2, где сделаны следующие переобозначения: $D = \tilde{Q} - \tilde{R}, E = trP - (\infty), m = N, k = \mathbb{F}_{r^{kw}}, w = ord_N r^k$):

$$\varepsilon(\tilde{Q}, trP) = \left(\frac{f'_{N,\tilde{Q}}(trP)}{f'_{N,\tilde{Q}}(\infty)}\right)^{\frac{r^{wk}-1}{N}}$$

для любых $P, Q \in E(\mathbb{F}_{r^k})$. Пусть $v = ord_N T$, а $L \in \mathbb{N}$ определено равенством $LN = T^v - 1$. Докажем, что формула (8) задаёт билинейное отображение $(E(\mathbb{F}_{r^k}))^2 \to \mathbb{F}^*_{r^{kw}}/(\mathbb{F}^*_{r^{kw}})^N$, нетривиальное на $G_2 \times G_1$. Доказательство проводится по плану [18]. Имеем

$$\varepsilon(\tilde{Q}, trP)^L = \left(\frac{f'_{LN,\tilde{Q}}(trP)}{f'_{LN,\tilde{Q}}(\infty)}\right)^{\frac{r^{wk}-1}{N}} = \left(\frac{f'_{T^v-1,\tilde{Q}}(trP)}{f'_{T^v-1,\tilde{Q}}(\infty)}\right)^{\frac{r^{wk}-1}{N}} = \left(\frac{f'_{T^v,\tilde{Q}}(trP)}{f'_{T^v,\tilde{Q}}(\infty)}\right)^{\frac{r^{wk}-1}{N}}. \tag{9}$$

Последнее равенство верно, так как, по построению, $T^v \equiv 1(modN)$, и

$$(T^v\tilde{Q}) = \tilde{Q}, ((T^v - 1)\tilde{Q}) = (\infty).$$

Согласно Лемме 2 [22], имеем

$$f_{T^v,\tilde{Q}} = f_{T,\tilde{Q}}^{T^{v-1}} f_{T,T\tilde{Q}}^{T^{v-2}} \cdots f_{T,T^{v-1}\tilde{Q}}.$$

Аналогично это же будет верно с заменой $\tilde{Q}$ на $\tilde{R}$. Применяя свойства отображения $\tilde{Q}(Q)$, получим $[T]\tilde{Q} = \pi_r^j\tilde{Q}, [T]\tilde{R} = \pi_r^j\tilde{R}$. Заметим, что при $P \in E(\mathbb{F}_{r^k})$

$$\frac{f_{T,T^l\tilde{Q}}(trP)}{f_{T,T^l\tilde{R}}(trP)} = \frac{f_{T,\pi_r^{jl}\tilde{Q}}(trP)}{f_{T,\pi_r^{jl}\tilde{R}}(trP)} = \left(\frac{f_{T,\tilde{Q}}(trP)}{f_{T,\tilde{R}}(trP)}\right)^{r^{jl}},$$

поэтому

$$f'_{T^v,\tilde{Q}}(trP) = (f'_{T,\tilde{Q}}(trP))^{\sum_{l=0}^{v-1} T^{v-1-l}r^{jl}} = (f'_{T,\tilde{Q}}(trP))^M, M = \frac{r^{jv} - T^v}{r^j - T}.$$

Аналогично это же будет верно с заменой trP на (∞), так как коэффициенты кривой лежат в $\mathbb{F}_r$. Таким образом, из (9) имеем

$$(\varepsilon(\tilde{Q}, trP))^L = (\tilde{e}_T(Q, P))^{M\frac{r^{wk}-1}{N}}. \tag{10}$$

Справедливость этого равенства была проверена численно, однако дальнейшее использование рассматриваемого спаривания в нашем алгоритме, при

$$(L, p) = 1,$$

стало невозможным из-за слишком малой вероятности обращения уравнения

$$\tilde{e}_T(Q, P) = z\tilde{z}^N, \tag{11}$$

при случайном выборе $\tilde{z}^N \in \mathbb{F}_{r^k}$.

5. Основной вариант спаривания

В этом разделе сконструтровано новое спаривание, с предположительно более высокой вероятностью обращения равенства вида (11) при случайном выборе $\tilde{z}^N \in \mathbb{F}_{r^k}$. В подтверждение этого проведено сравнение мощностей сдвига и свободных компонент аргументов.

При подстановке в качестве $N = \sharp E(\mathbb{F}_{r^k})$ спаривание ε для выбранной эллиптической кривой при подстановке точек из $E(\mathbb{F}_{r^k})$ оказалось тождественно равно единице. В предлагаемом нами примере универсальная экспонента $\Sigma = \Sigma(E(\mathbb{F}_{r^k}))$ группы точек $E(\mathbb{F}_{r^k})$ является делителем числа N. Оказалось, что если вместо N подставить универсальную экспоненту, то рассматриваемое спаривание при подстановке точек из $E(\mathbb{F}_{r^k})$ уже не является тождественной единицей. Поскольку основным объектом наших исследований далее является нередуцированное Σ спаривание Тейта, то результаты дальнейших исследований мы будем формулировать для него. Будем обозначать его ε'.

Применяя к спариванию Тейта с универсальной экспонентой процедуру понижения степени, было получено новое спаривание $\tilde{e}_T$, выражающееся рациональной функцией малой степени. Оно определено на всех точках из $E(\mathbb{F}_{r^k})$. При условии $p \nmid L$ это спаривание, как

и ожидалось, оказалось невырожденным на $G_2 \times G_1$, однако вероятность разрешимости уравнений эквивалентных его обращению оказалась слишком низкой. Причина этого в присутствии сжимающих отображений $tr, \tilde{Q}$ в результате действия которых мощность образа рассматриваемого нередуцированного спаривания существенно меньше, чем порядок мультипликативной группы $\mathbb{F}^*_{r^k}$, в которой для решения задачи обращения предполагалось выбирать элемент при помощи случайного выбора представителя смежного класса. Таким образом для повышения этой вероятности возникла необходимость корректировки конструкции используемого спаривания, чтобы рассматриваемая процедура понижения степени работала при условии произвольности (или почти произвольности) его аргументов в $E(\mathbb{F}_{r^k})$ и приводила к невырожденному на $G_2 \times G_1$ спариванию.

Наше желание использовать нередуцированное спаривание Тейта обосновано тем, что, согласно полученной нами выше Теореме 2, оно отличается от редуцированного, только наличием сдвига и, по существу ничего не меняющим, возведением в степень других компонент результата. При этом, отсутствие редуцирующей степени делает задачу обращения этого спаривания намного более простой. Мы будем пользоваться Теоремой 2 вместо Теоремы 3 [17].

Если при некоторой фиксированной компоненте из $\tilde{G}_1$ (см. Теорему 2), некотором сдвиге и фиксированном одном (первом или втором) аргументе спаривание ε' обратимо по другому аргументу, то для получения существенной компоненты этого аргумента, принадлежащей G_2 или G_1 применяется сжимающее отображение

$$[(1-r)^{-1} \pmod p](\pi - [r])\left[\left(\frac{\Sigma}{p}\right)^{-1} \pmod p\right]\left[\frac{\Sigma}{p}\right],$$

для получения компоненты из G_1, или

$$[(r-1)^{-1} \pmod p](\pi - [1])(\left[\left(\frac{\Sigma}{p}\right)^{-1} \pmod p\right]\left[\frac{\Sigma}{p}\right],$$

для получения компоненты из G_2, соответственно.

Таким образом осталось решить задачу обращения в элементы, лежащие в $E(\mathbb{F}_{r^k})$. Для этого используемое спаривание должно быть представлено рациональной функцией малой степени и принимать «почти» все возможные значения в $\mathbb{F}_{r^k}$, чтобы случайный выбор сдвига с хорошей вероятностью приводил к разрешимому уравнению.

Для сохранения свойств линейности, невырожденности и широкой области определения Σ спаривания Тейта ε' при процедуре понижения степени предлагается следующая его модификация. Пусть

$$T \equiv r^j \pmod \Sigma, \tag{12}$$

$(j,k) = k_0$. Будем считать, что величина T полиномиально зависит от $\log p$. Кривые с одновременно малыми значениями T и k получатся если взять, например, простые p и r так, что $p \mid T^k - 1, r = p + T$ (можно перебирать T и k, проверяя на простоту получающееся r). Тогда вероятность выполнения равенства (12) представляется достаточно высокой. Кривая с такими параметрами существует по известной теореме Ваттерхауза [23], хотя алгоритма, который бы мог её построить пока нет.

Рассмотрим спаривание, заданное формулой

$$\prod_{l=0}^{\frac{k}{k_0}} f_{\Sigma,Q}(P^{\pi^{lk_0}}).$$

Здесь мы учли то, что в результате численных экспериментов выяснилось, что алгоритм Миллера выдаёт функцию $f_{N,Q}(P)$ в нормированном виде (то есть она равна единице при подстановке бесконечной точки вместо любого из аргументов). Поэтому спаривание Тейта, например, можно записать просто $\varepsilon(Q,P) = f_{N,Q}(P)$.

Аналогично уже рассмотренной ранее процедуре понижения степени при $T^v - 1 = L\Sigma$, получим

$$\left(\prod_{l=0}^{\frac{k}{k_0}} f_{\Sigma,Q}(P^{\pi^{lk_0}})\right)^L = \prod_{l=0}^{\frac{k}{k_0}} f_{T^v,Q}(P^{\pi^{lk_0}}) =$$

$$= \prod_{l=0}^{\frac{k}{k_0}} f_{T,Q}(P^{\pi^{lk_0}}) \prod_{l=0}^{\frac{k}{k_0}} f_{T,[T]Q}(P^{\pi^{lk_0}}) \cdots \prod_{l=0}^{\frac{k}{k_0}} f_{T,[T^{v-1}]Q}(P^{\pi^{lk_0}}) = \left(\prod_{l=0}^{\frac{k}{k_0}} f_{T,Q}(P^{\pi^{lk_0}})\right)^M.$$

с тем же самым значением $M = \frac{r^{jv}-T^v}{r^j-T}$, но уже при всех $P \in E(\mathbb{F}^*_{r^k})$ и $Q \in E(\mathbb{F}^*_{r^k}) \cap \ker(\pi - [r])$.

Обозначая новое спаривание $\varepsilon''(Q,P) = \prod_{l=0}^{\frac{k}{k_0}} f_{T,Q}(P^{\pi^{lk_0}})$, при $p \nmid L$ получим для него те же свойства, что и для ε', а именно выполнение утверждения Теоремы 2.

Пусть теперь требуется обратить рассматриваемое спаривание по первому аргументу. В этом случае исключение переменной y (второй координаты точки Q) из системы, состоящей из уравнения кривой и уравнения

$$\varepsilon''(Q,P) = z\tilde{z}, z \in \tilde{G}_1, \tag{13}$$

ввиду малости параметров k, T приводит, как и выше, к решению многочлена от одной переменной относительно малой степени.

Пусть теперь требуется обратить рассматриваемое спаривание по второму аргументу. В этом случае в рассматриваемые уравнения входят не только неизвестные координаты точки P, лежащие в $\mathbb{F}_{r^k}$, но и величины, полученные из них применением автоморфизма Фробениуса. Поэтому предлагается некоторая новая процедура, сводящая данную задачу к решению системы линейных уравнений.

Исключая степени, старше первой, переменной y с помощью уравнения кривой, получим

$$f_{T,Q}(P(x,y)) = \frac{yf_{11} + f_{12}}{yf_{21} + f_{22}}.$$

Пусть

$$yf_{11} + f_{12} = \sum_{i=0,1,\ldots,S-1;j=0,1} a_{ij}x^i y^j,$$

$$yf_{21} + f_{22} = \sum_{i=0,1,\ldots,S-1;j=0,1} b_{ij}x^i y^j.$$

Тогда уравнение (13) можно записать в виде

$$\prod_{l=0}^{\frac{k}{k_0}} \sum_{i=0,1,\ldots,S-1;j=0,1} a_{ij} {x_l}^i {y_l}^j = z \prod_{l=0}^{\frac{k}{k_0}} \sum_{i=0,1,\ldots,S-1;j=0,1} b_{ij} {x_l}^i {y_l}^j, \tag{14}$$

где x_l, y_l координаты точки $P^{\pi^{lk_0}}$. Раскрывая скобки, получим

$$\prod_{l=0}^{\frac{k}{k_0}} \sum_{i=0,1,\ldots,S-1;j=0,1} a_{ij} {x_l}^i {y_l}^j = \sum_{\psi} c_\psi \psi(x_1, y_1, \ldots, x_{\frac{k}{k_0}}, y_{\frac{k}{k_0}}), \tag{15}$$

где c_ψ - все различные произведения вида $\prod_{i,j} {a_{ij}}^{\alpha_{ij}}, \alpha_{ij} \in \mathbb{N} \cup \{0\}, \sum_{i,j} \alpha_{ij} = \frac{k}{k_0}$, а ψ - некоторые многочлены от $2\frac{k}{k_0}$ переменных. Количество таких произведений (а значит и многочленов ψ не больше чем $C^{2S-1}_{\frac{k}{k_0}+2S-1} \leq (\frac{k}{k_0} + 2S)^{2S-1}$. Как уже неоднократно отмечалось (см. например [10]), равенство $T \equiv r^j \pmod p$ приводит к тому, что $T^k \approx p$. Однако, если выбрать S, T небольшими константами, а $k \approx \log p$, то количество многочленов ψ оценится небольшой величиной k^{2S}. Подставляя выражение (15) и аналогичное ему выражение для правой части в уравнение (14), получим линейное однородное уравнение от переменных ψ. Заменяя в равенстве (13) P на $[m]P$, а z на z^m для различных значений m, аналогично получим другие линейные однородные уравнения для тех же переменных ψ. Решая полученную систему за $O((\log p)^{6S})$ арифметических опрераций получим все переменные ψ с точностью до мультипликативной константы C. Поскольку $f(\lambda) = \prod_l (\lambda - x_l)$ при фиксированном λ также имеет вид (15), мы получим его с точностью до умножения на C. Выбирая $\frac{k}{k_0}$ различных значений для λ, по интерполяционной формуле Лагранжа получим многочлен $Cf(x) \in \mathbb{F}_{r^k}[x]$ среди корней которого найдем искомое нами решение.

Осталось оценить вероятность разрешимости уравнения (13) при случайном выборе $\tilde{z}$. В случае обращения по второму аргументу (то есть при фиксированном Q) искомое значение $P \in G_1$ может быть «сдвинуто» при помощи любых значений остальных компонент разложения группы $E(\mathbb{F}_{r^k})$. Мощность такого «сдвига» оценивается величиной $\sharp E(\mathbb{F}_{r^k}) / \sharp G_1 \approx \frac{r^k}{r}$. В тоже время мощность возможных $\tilde{z}$ оценивается такой же величиной. При этом, если Q лежит в G_2 надо компоненты $\tilde{z}$, лежащие в примарных компонентах $\tilde{G}_i, i \geq 2$, соответствующих простым p_i из разложения НОД$(\sharp E(\mathbb{F}_{r^k})[N], r^k - 1)$ (см. Теорему 2) равными единице. В случае, если мы прибавим к Q произвольную точку из $\ker(\pi - [r])$ с нулевой компонентой, соответствующей G_2, этого обнуления можно не делать.

В случае обращения уравнения (13) по первому аргументу (то есть при фиксированном P) искомое значение $Q \in G_2$ может быть «сдвинуто» при помощи любых значений остальных компонент разложения группы $E(\mathbb{F}_{r^k}) \cap \ker(\pi - [r])$. Мощность такого «сдвига» оценивается величиной $\sharp E(\mathbb{F}_{r^k}) / (\sharp \ker(\pi - [1]) \sharp G_2) \approx \frac{r^k}{rp}$. В тоже время мощность возможных $\tilde{z}$ оценивается такой величиной $\frac{r^k}{p \prod p_i}$, где произведение берётся по $i \geq 2$, для которых p_i делит НОД$(\sharp E(\mathbb{F}_{r^k})[N], r^k - 1)$, поскольку при $P \in G_1$ компоненты $\tilde{z}$, лежащие в примарных компонентах $\tilde{G}_i, i \geq 2$, соответствующих простым p_i из разложения НОД$(\sharp E(\mathbb{F}_{r^k})[N], r^k - 1)$ (см. Теорему 2) равны единице и количество таких различных $\tilde{z}$ оценивается величиной $\frac{r^k}{p \prod p_i}$, где произведение берётся по $i \geq 2$, для которых p_i делит НОД$(\sharp E(\mathbb{F}_{r^k})[N], r^k - 1)$. Такие i для некоторых кривых существуют (см. табл. 3).

Таким образом существуют кривые, для которых случайный выбор $\tilde{z}$ при обращении равенства (13) может оказаться эффективным если значительная доля сдвигов образа может быть получена при помощи сдвигов прообразов, относительно соответственно G_2 и

G_1. Поскольку мощности этих сдвигов близки этому может помешать только «слипание» сдвигов прообразов рассматриваемого спаривания в один сдвиг образа. Однако, поскольку наше спаривание задаётся рациональной функцией малой степени, это не может привести к существенному снижению рассматриваемой вероятности разрешимости уравнения (13).

Список литературы

[1] Menezes A., Okamoto T., Vanstone S. Redusing elliptic curve logarithms in a finite field. IEEE Trans. Inf. Theory, vol.IT-39, no.5, pp.1639-1646, 1993.

[2] Verheul E.R. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. J. Cryptology, 17, 277-296 (2004). doi: 10.1007/s00145-004-0313-x

[3] Takakazu Satoh Miller is Easy for the Redused Tate Pairing on Supersingular Curves of Embedding Degree Two and Three. https://eprint.iacr.org/2019/385

[4] Akagi S., Nogami Y. Exponentiation inversion problem redused from fixed argument pairing inversion on twistable Ate pairing and its difficulty. Advances in Information and ComputerSecurity. IWSEC 2014, Lect. Notes in Comput. Sci., 8639, p.240-249

[5] Barreto P.S.L.M., Naehrig M. Pairing-friendly elliptic curves of prime order. SAC 2005, Lect. Notes in Comput. Sci., 3897, p.319-331

[6] Bresing F., Weng A. Ellcurves suitable for pairing based cryptography. Des. Codes Crypt., 37, 2005, p.133-141

[7] Freeman D. Constructing pairing-friendly ellcurves with embedding degree 10. Algorithmic Number Theory, Proc. 7th Internat. Sympo, ANTS-VII 2006, Lect. Notes in Comput. Sci., 4076, p.452-465

[8] Dupont R., Enge A., Morain F. Building curves with arbitrary small MOV-degree over finite prime fields. J.Cryptol., 18(2005), p.79-89. http://eprint.iacr.org/2002/094.pdf

[9] Silverman J. The Arithmetic of Elliptic Curves.-Springer,1986.-513+xviiip.

[10] Черепнев М.А. Обращение спариваний для решения задачи дискретного логарифмирования. Фундаментальная и прикладная математика 2013, Т.18, Вып.4, стр.185-195. Journal of Mathematical Science: Volume 206, Issue 6 (2015), page 734-741.

[11] Galbraith S., Hess F., Vercauteren F. Aspects of pairing invertion. IEEE Trans., Dec. 2008, v.54, Issue:12, p.5719-5728.

[12] Davenport J.H. On the integration of Algebraic Functions. LNCS 102 (1979), Springer-Verlag, Berlin

[13] Miller V.S. Short Programs for functions on Cyrves. Unpublished manuscript. 1986. http://crypto.stanford.edu/miller/

[14] Miller V.S. The Weil Pairing, and Its Efficient Calculation. J.Cryptology (2004), 17, p.235-261

[15] Cohen H., Frey G. ets. Handbook of Elliptic and Hyperelliptic curve Cryptography. Chapman and Hall, London, New York, Singapore 2006.

[16] Hess F. Pairing Lattices. In Pairing 2008, LNCS 5209, p. 18-38, Springer-Verlag, Berlin-Heidelberg-New York, 2008.

[17] Hess F. A Note on the Tate Pairing of Curves over Finite Fields. Arch. Math. (Basel)82 (2004), 28-32.

[18] F. Hess, N.P. Smart and F. Vercauteren. The Eta-pairing revisited. IEEE Transactions on Information Theory, vol 52, pages 4595-4602, Oct. 2006.

[19] Chang-An Zhao, Fangguo Zhang and Jiwu Huang A Note on the Ate Pairing Cryptology ePrint Archive: Report 2007/247. http://eprint.iacr.org/2007/247.pdf

[20] Василенко О.Н. Теоретико-числовые алгоритмы в криптографии.-М.:МЦНМО,2006.-325с.

[21] P.S.L.M.Barreto, C.Castello, R.Misoczki, M.Naehrig, G.C.C.F.Pereira, G.Zanon Subgroup security in pairing-based cryptography. Progress in Cryptology - LATINCRYPT 2015, LNCS 9230, Springer-Verlag (2015), pp.245-265 Cryptology ePrint Archive, Report 2015/247

[22] P.S.L.M.Barreto, S.Galbraith, C.Oh'Eigeartaigh, M.Scott Efficient Pairing Computation on Supersingular Abelian Varieties. Designs, Codes and Cryptography, Vol. 42, No. 3 (2007) 239-271.

[23] W. Watterhouse Abelian varieties over finite fields. Ann. Sci. Ecole Normale Sup. 4^{e} Serie 2 (1969), 521-560.