Спаривание Вейля и его применение к задачам Диффи—Хеллмана

М. И. Анохин

Спаривание Вейля является, по существу, невырожденным кососимметричным билинейным отображением на некоторой подгруппе группы точек эллиптической кривой. Определение спаривания Вейля можно найти во многих книгах, посвященных эллиптическим кривым (см., например, [6, 8, 2, 3]). Однако это определение опирается на большое количество понятий из алгебраической геометрии. Данный текст не требует от читателя предварительных знаний в области алгебраической геометрии, но предполагает наличие у него некоторой алгебраической подготовки.

Дальнейший материал организован следующим образом. В разделе 1 (к сожалению, получившемся довольно длинным) содержится минимальный объем сведений из алгебраической геометрии, необходимый для определения спаривания Вейля. Само это определение (в двух эквивалентных формулировках), а также основные свойства спаривания Вейля приводятся в разделе 2. В первых двух разделах мы предпочли не отвлекать читателя ссылками на литературу (ввиду стандартности материала), поэтому отметим, что при написании этих разделов использованы вышеупомянутые книги по эллиптическим кривым, а также книга [1] (на русском языке), хотя в ней и нет определения спаривания Вейля. Наконец, в разделе 3 показано, как в некоторых случаях эффективно вычислимое билинейное отображение (которое иногда может быть построено на основе спаривания Вейля) позволяет эффективно решать как распознавательную, так и вычислительную задачу Диффи—Хеллмана.

Отметим, что спаривания (в частности, спаривание Вейля) можно использовать не только для эффективного решения важных для криптографии вычислительных задач, но и для построения криптографических протоколов и примитивов. Эта тема исследований называется по-английски *pairing-based cryptography*; с ее основами можно познакомиться, в частности, в [2, Chapter X], [6, Section XI.7].

1. Необходимые сведения из алгебраической геометрии

Для произвольного кольца R через R^* будет обозначаться группа обратимых элементов этого кольца. Пусть K — произвольное совершенное поле, а $\overline{K}$ — его алгебраическое замыкание. (Напомним, что совершенность поля K означает, что либо характеристика K равна 0, либо она равна $p \neq 0$ и K содержит корень p-й степени из любого элемента этого поля.) *Эллиптической кривой* над K называется множество всех точек проективной плоскости над этим полем, однородные координаты $(X : Y : Z)$ которых удовлетворяют уравнению вида

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1}$$

где $a_1, a_2, a_3, a_4, a_6 \in K$. Напомним, что точка проективной плоскости над K — это класс троек из $K^3 \setminus \{(0,0,0)\}$ относительно эквивалентности, при которой w эквивалентно w' тогда и только тогда, когда $w' = \lambda w$ для некоторого $\lambda \in K^*$. Каждая такая точка задается набором однородных координат $(X : Y : Z)$, в котором $(X, Y, Z) \in K^3 \setminus \{(0,0,0)\}$, причем $(\lambda X : \lambda Y : \lambda Z) = (X : Y : Z)$ для любого $\lambda \in K^*$.

Уравнение (1) называется *уравнением Вейерштрасса*; множество всех его решений над K мы обозначаем через E. Мы будем иметь дело также с эллиптической кривой $\overline{E}$, заданной тем же уравнением (1), что и E, но на проективной плоскости над $\overline{K}$.

Легко видеть, что E состоит из множества всех точек $(x : y : 1)$, в которых $x, y \in K$ удовлетворяют уравнению

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2}$$

и точки $O = (0 : 1 : 0)$, называемой *бесконечно удаленной*. Хорошо известно, что на E можно ввести бинарную операцию, относительно которой эта кривая образует абелеву группу с нейтральным элементом O. Эту операцию мы здесь не определяем как ввиду громоздкости ее определения, так и в связи с тем, что ее явный вид нам не понадобится. Указанную группу мы будем записывать

аддитивно; кроме того, во избежание двусмысленности, l-кратное точки $P \in E$ в этой группе будет обозначаться через $[l]P$, а не lP. Здесь l может быть как целым числом, так и элементом $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, где n — порядок P как элемента группы E. Аналогичные рассуждения применимы к $\overline{E}$, содержащей E в качестве подгруппы.

Отметим, что если характеристика поля не равна ни 2, ни 3, то с помощью замены переменных уравнение (2) можно преобразовать к виду $y^2 = x^3 + bx + b'$, где $b, b' \in K$. Именно такие уравнения чаще всего рассматриваются в литературе по эллиптическим кривым.

Пусть f — однородный многочлен из $\overline{K}[x, y, z]$. Тогда очевидно, что если f обращается в 0 на какой-либо тройке $w \in \overline{K}^3$, то он обращается в 0 и на всех тройках вида λw, где $\lambda \in \overline{K}^*$. Поэтому корректны записи вида $f(P) = 0$ и $f(P) \neq 0$, где P — точка проективной плоскости над $\overline{K}$. Мы будем писать $f \equiv 0$ на $\overline{E}$, если $f(P) = 0$ для всех $P \in \overline{E}$ и $f \not\equiv 0$ на $\overline{E}$ в противном случае.

Рациональная функция на $\overline{E}$ может быть определена как класс формальных отношений f/g, где f и g — однородные многочлены из $\overline{K}[x, y, z]$ одной и той же степени (своей для каждой пары (f, g)), причем $g \not\equiv 0$ на $\overline{E}$, относительно следующего отношения эквивалентности:

$$f/g \approx u/v \iff fv - gu \equiv 0 \text{ на } \overline{E}.$$

Рациональные функции на $\overline{E}$ образуют поле относительно естественных для формальных отношений операций сложения и умножения. Это следует из того нетривиального факта, что если f и g — однородные многочлены из $\overline{K}[x, y, z]$, для которых $f \not\equiv 0$ и $g \not\equiv 0$ на $\overline{E}$, то и $fg \not\equiv 0$ на $\overline{E}$. Поле всех рациональных функций на $\overline{E}$ мы обозначаем через Φ. Его подполе $\left\{\lambda/1 \;\middle|\; \lambda \in \overline{K}\right\}$ естественно отождествляется с $\overline{K}$, поэтому Φ является также $\overline{K}$-алгеброй.

Слово «функция» в определении рациональной функции не означает, что она ставит в соответствие любой точке кривой $\overline{E}$ некоторый элемент поля $\overline{K}$. Пусть $P \in \overline{E}$. Если для $\varphi \in \Phi$ существует представление вышеуказанного вида f/g, где $g(P) \neq 0$, то φ называется *регулярной* в точке P. В этом случае корректно определено значение $\varphi(P) = f(w)/g(w) \in \overline{K}$, где $w \in \overline{K}^3$ — произвольный представитель точки P как класса эквивалентности. Рациональные функции на $\overline{E}$, регулярные в точке P, образуют локальную $\overline{K}$-подалгебру в Φ, обозначаемую нами через R_P. Единственный максимальный идеал этой подалгебры, обозначаемый через M_P, состоит из всех $\varphi \in R_P$ таких, что $\varphi(P) = 0$. Если $\tau \in M_P$, но τ не принадлежит второй степени идеала M_P (такая функция существует), то всякий элемент $\varphi \in \Phi^*$ может быть однозначно представлен в виде $\tau^n\psi$, где $n \in \mathbb{Z}$ и $\psi \in R_P \setminus M_P = R_P^*$. Число n в таком представлении не зависит от выбора τ и называется *порядком* φ в точке P; этот порядок будет обозначаться через $\operatorname{ord}_P \varphi$. Для $\varphi \in \Phi^*$ возможны три случая:

- Если $\operatorname{ord}_P \varphi > 0$, то $\varphi \in R_P$ и $\varphi(P) = 0$. В этом случае говорят, что φ имеет нуль порядка $\operatorname{ord}_P \varphi$ в точке P.
- Если $\operatorname{ord}_P \varphi = 0$, то $\varphi \in R_P$ и $\varphi(P) \in \overline{K}^*$. В этом случае $\varphi \in R_P^*$.
- Если $\operatorname{ord}_P \varphi < 0$, то $\varphi = \psi/\tau^{-\operatorname{ord}_P \varphi}$, где $\psi, \tau \in R_P$, $\psi(P) \neq 0$ и $\tau(P) = 0$. В этом случае полагают $\varphi(P) = \infty$ и говорят, что φ имеет полюс порядка $-\operatorname{ord}_P \varphi$ в точке P.

Таким образом, каждый элемент Φ^* можно считать функцией из $\overline{E}$ в $\overline{K} \cup \{\infty\}$.

Дивизором на $\overline{E}$ называется формальная сумма вида $\sum_{P \in \overline{E}} n_P(P)$, где n_P — целые числа, равные 0 для всех $P \in \overline{E}$, кроме конечного их числа. Другими словами, дивизоры на $\overline{E}$ — это элементы свободной абелевой группы с базисом $\left\{(P) \;\middle|\; P \in \overline{E}\right\}$. Пусть $D = \sum_{P \in \overline{E}} n_P(P)$ — дивизор на $\overline{E}$. *Степенью* $\deg D$ этого дивизора называется целое число $\sum_{P \in \overline{E}} n_P$. *Носитель* дивизора D — это множество всех $P \in \overline{E}$ таких, что $n_P \neq 0$. Для произвольной рациональной функции $\varphi \in \Phi^*$ ее дивизор $\operatorname{div} \varphi$ определяется как $\sum_{P \in \overline{E}} (\operatorname{ord}_P \varphi)(P)$. Это определение корректно, так как число точек $P \in \overline{E}$, для которых $\operatorname{ord}_P \varphi \neq 0$, конечно. Отображение div является гомоморфизмом группы Φ^* в группу дивизоров на $\overline{E}$ (относительно естественной операции сложения формальных сумм). Ядро этого гомоморфизма есть множество $\left\{\lambda/1 \;\middle|\; \lambda \in \overline{K}^*\right\}$. Дивизор на $\overline{E}$ называется *главным*, если он принадлежит образу гомоморфизма div. Известно, что

$$D \text{ — главный дивизор} \iff \deg D = 0 \text{ и } \sum_{P \in \overline{E}} [n_P]P = O \tag{3}$$

(последняя сумма берется в группе $\overline{E}$). Дивизоры D и D' на $\overline{E}$ называются *эквивалентными* ($D \sim D'$), если дивизор $D - D'$ является главным. Пусть $\varphi \in \Phi^*$, причем носители $\operatorname{div} \varphi$ и D не пересекаются. Тогда *значение* φ на D определено следующим образом:

$$\varphi(D) = \prod_{P \in \overline{E}} \varphi(P)^{n_P} \in \overline{K}^*,$$

где считается, что $0^0 = \infty^0 = 1$. Если $\deg D = 0$, то легко видеть, что $\varphi(D) = (\lambda\varphi)(D)$ для всех $\lambda \in \overline{K}^*$ и, следовательно, $\varphi(D)$ зависит лишь от дивизоров $\operatorname{div}\varphi$ и D.

Для произвольного целого положительного числа n через $E[n]$ ($\overline{E}[n]$) обозначается подгруппа группы E (соответственно, $\overline{E}$), состоящая из всех $P \in E$ (соответственно, $P \in \overline{E}$), для которых $[n]P = O$. Если это число n не делится на характеристику поля K, то $\overline{E}[n]$ является прямой суммой двух циклических подгрупп порядка n.

2. Определение и свойства спаривания Вейля

Фиксируем целое положительное число m, не делящееся на характеристику поля K. Пусть $S, T \in \overline{E}[m]$. Определим результат $e_m(S,T)$ *спаривания Вейля* на паре (S,T). Пусть T' — произвольная точка из $\overline{E}[m^2]$, для которой $[m]T' = T$ (легко видеть, что $\overline{E}[m] = [m]\left(\overline{E}[m^2]\right)$, так как $\overline{E}[m^2]$ — прямая сумма двух циклических подгрупп порядка m^2). Выберем какую-либо функцию $\varphi \in \Phi^*$, для которой

$$\operatorname{div}\varphi = \sum_{P \in \overline{E}[m]} (T' + P) - (P), \tag{4}$$

где $T' + P$ берется в группе $\overline{E}$, а остальные групповые операции — в группе дивизоров на $\overline{E}$. Согласно (3) такая функция φ существует (здесь также использовано то, что $\left|\overline{E}[m]\right| = m^2$). Кроме того, дивизор в правой части (4) не зависит от выбора T', так как он равен $\sum_{P \in \overline{E}[m^2] \mid [m]P = T}(P) - \sum_{Q \in \overline{E}[m]}(Q)$. Определим функцию ψ равенством $\psi(P) = \varphi(P + S)$ для всех $P \in \overline{E}$. Тогда $\psi \in \Phi^*$, причем $\operatorname{div}\psi = \operatorname{div}\varphi$. Следовательно, ψ/φ является константой из $\overline{K}^*$, которая и объявляется значением $e_m(S,T)$ (независимость $e_m(S,T)$ от выбора φ очевидна).

Приведем теперь основные свойства спаривания Вейля.

1) Билинейность: для любой точки $T \in \overline{E}[m]$ отображения $P \mapsto e_m(P,T)$ и $P \mapsto e_m(T,P)$ ($P \in \overline{E}[m]$) являются гомоморфизмами из $\overline{E}[m]$ в $\overline{K}^*$. В частности, e_m отображает $\overline{E}[m] \times \overline{E}[m]$ в группу всех корней m-й степени из 1 в $\overline{K}$.

2) Кососимметричность: $e_m(P,P) = 1$ для всех $P \in \overline{E}[m]$. Следовательно, $e_m(T,S) = e_m(S,T)^{-1}$ при любых $S, T \in \overline{E}[m]$.

3) Невырожденность: если для $T \in \overline{E}[m]$ равенство $e_m(P,T) = 1$ (или, что эквивалентно, $e_m(T,P) = 1$) справедливо при всех $P \in \overline{E}[m]$, то $T = O$.

4) Если σ — автоморфизм поля $\overline{K}$, тождественный на K, то $e_m(\sigma(S), \sigma(T)) = \sigma(e_m(S,T))$ для всех $S, T \in \overline{E}[m]$. (Здесь σ действует на точки проективной плоскости над $\overline{K}$ покоординатно и отображает $\overline{E}[m]$ на себя.) В частности, e_m отображает $E[m] \times E[m]$ в K.

5) Если m' — целое положительное число m, не делящееся на характеристику поля K, то $e_{mm'}(S,T) = e_m([m']S, T)$ при любых $S \in \overline{E}[mm']$ и $T \in \overline{E}[m]$.

Имеется эквивалентное определение спаривания Вейля, которое позволяет построить эффективный алгоритм для его вычисления (основанный на алгоритме Миллера, см. [5], [6, Section XI.8], [8, Section 11.4], [2, Section IX.8]). А именно, пусть $S, T \in \overline{E}[m]$. Выберем произвольные дивизоры A и B на $\overline{E}$, имеющие нулевую степень, непересекающиеся носители и такие, что $A \sim (S) - (O)$ и $B \sim (T) - (O)$. Согласно (3) мы можем выбрать функции $\varphi, \psi \in \Phi^*$ такие, что $\operatorname{div}\varphi = mA$ и $\operatorname{div}\psi = mB$. Тогда $e_m(S,T) = \varphi(B)/\psi(A)$.

3. Применение билинейных отображений к решению задач Диффи—Хеллмана

В настоящем разделе мы предполагаем, что поле K выбирается из бесконечного эффективно заданного семейства конечных полей. В этом случае спаривание Вейля эффективно вычислимо с помощью алгоритма, основанного на алгоритме Миллера (см. ссылки в конце предыдущего раздела). Пусть $P \in E$, а n — порядок P как элемента группы E. Под *распознавательной задачей Диффи—Хеллмана* по основанию P мы понимаем задачу проверки по $(P, [a]P, [b]P, [c]P)$ $(a, b, c \in \mathbb{Z}_n)$ истинности равенства $[ab]P = [c]P$ (которое равносильно равенству $ab = c$ в $\mathbb{Z}_n$). *Вычислительная задача Диффи—Хеллмана* по основанию P — это задача вычисления по $(P, [a]P, [b]P)$ $(a, b \in \mathbb{Z}_n)$ элемента $[ab]P$. Разумеется, описания поля K и эллиптической кривой (с помощью уравнения вида (1) или (2)) также предполагаются известными.

Следующий подход принадлежит Жу и Нгуену [4] (см. также [8, Section 6.2]). Предположим, что существует эффективно вычислимое билинейное отображение β на подгруппе $\langle P\rangle$, порожденной элементом P, принимающее значения в некоторой эффективно заданной группе и такое, что $\beta(P,P)$ имеет тот же порядок n, что и P. Тогда легко видеть, что

$$ab = c \text{ в } \mathbb{Z}_n \iff \beta([a]P,[b]P) = \beta([c]P,P)$$

для произвольных $a,b,c \in \mathbb{Z}_n$. Это позволяет эффективно решать распознавательную задачу Диффи—Хеллмана по основанию P. Рассмотрим теперь вопрос о возможности построения такого отображения β. Если $P \in E[m] \setminus \{O\}$, то в качестве β нельзя взять спаривание Вейля e_m, так как $e_m(P,P) = 1$. Однако можно попытаться найти эффективно вычислимый гомоморфизм α группы E в группу $\overline{E}$ такой, что билинейное отображение $(S,T) \mapsto e_m(S,\alpha(T))$ $(S,T \in \langle P\rangle,\ P \in E[m])$ обладает требуемым свойством. Вопрос о существовании такого гомоморфизма α остается открытым, за исключением некоторых частных случаев. Приведем пример (см. [8, Section 6.2]). Пусть эллиптическая кривая E задана уравнением $y^2 = x^3 + 1$ вида (2) над полем $K = \mathbb{F}_q$, где $q \equiv 2 \pmod 3$. Так как $q^2 - 1$ делится на 3, в $\mathbb{F}_{q^2}^*$ можно выбрать элемент ξ порядка 3. Тогда $\alpha\colon \overline{E} \to \overline{E}$ определяется следующим образом:

$$\alpha(x : y : 1) = (\xi x : y : 1), \quad \alpha(O) = O.$$

Можно показать, что α — автоморфизм группы $\overline{E}$. Кроме того, если m не делится на 3 и $P \in E$ имеет порядок m, то и $e_m(P,\alpha(P))$ имеет порядок m. (Напомним, что m предполагается взаимно простым с q.)

Предположим теперь, что существует эффективно вычислимое билинейное отображение δ на $\langle P\rangle$, принимающее значения в $\langle P\rangle$ и такое, что $\delta(P,P)$ порождает $\langle P\rangle$. В частности, таким отображением является $(S,T) \mapsto \gamma(\beta(S,T))$ $(S,T \in \langle P\rangle)$, где β обозначает то же, что и в начале предыдущего абзаца, а γ — эффективно вычислимый изоморфизм группы $\langle \beta(P,P)\rangle$ на группу $\langle P\rangle$ (разумеется, при условии существования таких β и γ). Кроме того, мы предполагаем известным некоторое целое число $k \geq 3$, делящееся на экспоненту группы $\mathbb{Z}_n^*$ (т. е. такое, что $d^k = 1$ для любого $d \in \mathbb{Z}_n^*$). Используя подход, принадлежащий Верхёлу [7] (см. также [2, Theorem IX.24]), покажем, как в этом случае можно эффективно решать вычислительную задачу Диффи—Хеллмана по основанию P. Пусть $c \in \mathbb{Z}_n$ таково, что $\delta(P,P) = [c]P$. Тогда $c \in \mathbb{Z}_n^*$. Очевидно, что $\delta([a]P,[b]P) = [abc]P$ для любых $a,b \in \mathbb{Z}_n$. Хотя значение c нам неизвестно, мы можем эффективно вычислять $[c^i]P$ по P и целому положительному числу i. Действительно, положим $Q_i = ([c^{i-1}]P,[c^i]P)$. Тогда пара $Q_1 = (P,\delta(P,P))$ вычисляется эффективно по P, а если уже известна пара Q_i, то Q_{2i} и Q_{2i+1} эффективно вычисляются следующим образом:

$$\begin{aligned} Q_{2i} &= (\delta([c^{i-1}]P,[c^{i-1}]P), \delta([c^{i-1}]P,[c^i]P)), \\ Q_{2i+1} &= (\delta([c^{i-1}]P,[c^i]P), \delta([c^i]P,[c^i]P)). \end{aligned}$$

Следовательно, по P и i можно эффективно вычислить Q_i и, в частности, $[c^i]P$. Для дальнейшего нам потребуется вычислить элемент $[c^{-2}]P = [c^{k-2}]P$, где c^{-2} берется в группе $\mathbb{Z}_n^*$. Тогда по $(P,[a]P,[b]P)$, где $a,b \in \mathbb{Z}_n$, элемент $[ab]P$ эффективно вычисляется как $\delta(\delta([c^{-2}]P,[a]P),[b]P)$.

Отметим, что методы решения задач Диффи—Хеллмана, описанные в настоящем подразделе, применимы не только к группам точек эллиптических кривых, но и к группам из произвольного бесконечного эффективно заданного семейства конечных групп.

Литература

[1] С. А. Степанов. Арифметика алгебраических кривых. М., Наука, Физматлит, 1991.

[2] I. F. Blake, G. Seroussi, N. P. Smart (eds.). Advances in elliptic curve cryptography. Cambridge University Press, 2005 (London Mathematical Society Lecture Note Series, 317).

[3] I. F. Blake, G. Seroussi, N. P. Smart. Elliptic curves in cryptography. Cambridge University Press, 1999.

[4] A. Joux, K. Nguyen. Separating Decision Diffie-Hellman from Computational Diffie-Hellman in cryptographic groups. J. Cryptology, v. 16, no. 4, p. 239–247, 2003.

[5] V. S. Miller. The Weil pairing, and its efficient calculation. J. Cryptology, v. 17, no. 4, p. 235–261, 2004.

[6] J. H. Silverman. The arithmetic of elliptic curves. 2nd ed. Springer Science+Business Media, LLC, 2009 (Graduate Texts in Mathematics, 106).

[7] E. R. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. J. Cryptology, v. 17, no. 4, p. 277–296, 2004.

[8] L. C. Washington. Elliptic curves: number theory and cryptography. 2nd ed. Taylor & Francis Group, LLC, 2008 (Discrete Mathematics and its Applications, 50).