УДК 512.77

М. В. Алешникова, С. И. Алешников
А. А. Горбачёв, Д. О. Олефиренко

УСКОРЕНИЕ ВЫЧИСЛЕНИЙ В ЯКОБИАНЕ ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Предложен метод ускорения процедур сложения и удвоения точек якобиана гиперэллиптической кривой в аффинных и проективных координатах. Разработаны соответствующие модификации алгоритма Миллера. В аффинных координатах затраты на групповую операцию удвоения больше затрат на групповую операцию сложения, поэтому выгоднее выполнить последовательно два сложения, чем удвоение и сложение. Получены оценки эффективности модифицированных алгоритмов.

In article is stated the method of acceleration of procedures of addition and doubling points Jacobian of a hyperelliptic curve in affine and projective coordinates. Corresponding modified Miller algorithms are developed. In affine coordinates an expense for group operation of doubling there are more than expenses for group operation of addition, therefore it is more favorable to realize consistently two additions, than doubling and addition. Estimations of efficiency of the modified algorithms are received.

Ключевые слова: гиперэллиптическая кривая, якобиан, сложение и удвоение дивизоров, алгоритм Миллера, проективные координаты.

Keywords: hyperelliptic curve, Jacobian, addition and doubling of divisors, Miller's algorithm, projective coordinates.

В настоящее время билинейные спаривания превратились в один из главных инструментов построения эффективных открытых систем защиты информации на эллиптических и гиперэллиптических кривых. Протоколы на основе спариваний стали активно использоваться в связи с появлением так называемых неинтерактивных протоколов [1] распределения ключей, трехсторонних протоколов обмена ключами [2], IB-шифрования. Для реализации протоколов со спариваниями требуются эффективные пути вычисления самих спариваний.

Уже разработано довольно много алгоритмов, осуществляющих быстрые вычисления спариваний. В работе [3] представлены явные формулы для групповых операций на кривых рода 2 с использованием различных систем координат. В [4] предыдущие формулы модифицированы для аффинных координат с целью уменьшения затрат на получение рациональных функций, требуемых в алгоритме Миллера. Хороший эффект дает использование эффективных автоморфизмов [5—7]. В работе [8] представлены явные формулы ускорения сложения одного дивизора с удвоенным другим, но не рассмотрено, как это отразится на работе алгоритма Миллера.

В [9] показано, что, даже обеспечивая высокий уровень секретности (такой, как при длине ключа 192 или 256 бит), вычисление спаривания Вейля может иногда происходить быстрее, нежели спаривания Тейта.

Дальнейший прогресс состоял в исследовании специальных классов гиперэллиптических кривых [10] и специального вида спариваний [11]. В частности, в [12] установлено, что для некоторых гиперэллиптических кривых с высокой степенью кручения вычисление спаривания Вейля может быть более быстрым, чем спаривания Тейта, *ate* и ate_i.

В настоящей работе рассматривается метод ускорения вычислений за счет изменения процедур сложения точек якобиана гиперэллиптической кривой в аффинных координатах. Описана соответствующая модификация алгоритма Миллера. Приведены оценки эффективности модифицированного алгоритма.

Пусть $\mathbf{F}_q$ — конечное поле с числом элементов q. Гиперэллиптическая кривая C рода $g \geq 1$ над $\mathbf{F}_q$ есть гладкая плоская кривая с уравнением

$$y^2 + h(x)y = f(x),$$

где $f(x)$ — унитарный многочлен степени $2g + 1$; $h(x)$ — многочлен степени, не превосходящей g.

Множество $C(\mathbf{F}_{q^k})$ точек кривой C с координатами в расширении $\mathbf{F}_{q^k}$ степени k для $g \geq 2$ не образует группы, однако C можно вложить в абелево многообразие J_C размерности g, называемое якобианом C. Это многообразие изоморфно группе Pic_C^0 классов дивизоров степени нуль, называемой группой Пикара. Якобиан кривой C над $\mathbf{F}_{q^k}$ обозначается $J_C(\mathbf{F}_{q^k})$, он изоморфен группе классов дивизоров степени нуль $\mathrm{Pic}_C^0(\mathbf{F}_{q^k})$ на C, определенных над $\mathbf{F}_{q^k}$.

Пусть $\overline{D} \in J_C(\mathbf{F}_q)$. В классических алгоритмах Кантора для сложения и удвоения дивизоров не рассматривается случай, когда дивизор D в координатах Мамфорда имеет вид $D = [a(x), b(x)]$, где $\deg a(x) < 2$. Модифицированный алгоритм позволяет устранить этот недостаток. Итак, пусть $D_1 = [u_1, v_1]$, $D_2 = [u_2, v_2]$ — редуцированные дивизоры. Рассмотрим различные случаи.

1. $\deg(u_1) = \deg(u_2) = 1$, $\deg(v_1) = \deg(v_2) = 0$.

1.1. Если $u_1 = u_2$, $v_1 = -v_2$, то $D_1 = -D_2$. При этом результатом их сложения будет $D_1 + D_2 = 0 = [1, 0]$ — нулевой элемент якобиана.

1.2. Если $u_1 = u_2$, $v_1 = v_2$, то речь идет об удвоении: $D_1 + D_2 = 2D_1$. Алгоритм удвоения с подсчетом числа арифметических операций представлен в таблице 1.

Таблица 1

Алгоритм удвоения

Вход: $D_1 = [x + u_{10}, v_{10}]$ Выход: $D_3 = [x^2 + u_{31}x + u_{30}, v_{31}x + v_{30}] = 2D_1$	Число операций
Вычисление коэффициентов u_3: $s_3 = (2 \cdot v_{10})^{-1}$, $u_{31} = 2u_{10}$, $u_{30} = u_{10}^2$	$M + I$, M, S

Окончание табл. 1

Вход: $D_1 = [x + u_{10}, v_{10}]$ Выход: $D_3 = [x^2 + u_{31}x + u_{30}, v_{31}x + v_{30}] = 2D_1$	Число операций
Вычисление коэффициентов v_3: $r_1 = u_{31}^2$, $r_2 = u_{30}^2$, $v_{31} = s_3(f_1 + 3u_{30}f_3 + 5r_2 - r_1u_{10}f_4 - u_{31}f_2)$, $v_{30} = (v_{10}^2 + r_1u_{30} + f_0 - u_{30}f_2 - 3r_2f_4 + u_{31}u_{30}f_3)s_3$	$2S$, $7M$, $7M + S$
Итого	$I + 16M + 4S$

Примечание: M — умножение; S — возведение в квадрат; I — инверсия.

Полагаем $u_1 = u_2 = x + u_{10}$, $v_1 = v_2 = x_{10}$. Имеем

1.2.1. $d_1 = \text{НОД}(u_1, u_2) = u_1$, поскольку наибольшим общим делителем двух равных многочленов является один из них. Тогда $d_1 = 0 \cdot u_1 + 1 \cdot u_2$. Полагаем $e_1 = 0$, $e_2 = 1$.

1.2.2. $d = \text{НОД}(d_1, v_1 + v_2) = 1$, поскольку d_1 — унитарный многочлен, имеем $\deg(d_1) = 1$, $\deg(v_1 + v_2) \le 0$. Тогда $1 = 0 \cdot d_1 + (2 \cdot v_{10})^{-1} \cdot (v_1 + v_2)$. Полагаем $c_1 = 0$, $c_2 = (2 \cdot v_{10})^{-1}$.

1.2.3. $s_1 = c_1 \cdot e_1 = 0$, $s_2 = c_1 \cdot e_2 = 0$, $s_3 = c_2$.

1.2.4. $u_3 = \dfrac{u_1u_2}{d^2} = \dfrac{u_1^2}{1} = u_1^2 = (x + u_{10})^2 = x^2 + 2 \cdot u_{10} + u_{10}^2$.

1.2.5. $v_3 = \dfrac{s_1u_1v_2 + s_2u_2v_1 + s_3(v_1v_2 + f)}{d} \bmod u_3 = s_3(v_{10}^2 + f) \bmod u_3$.

Получается, многочлен степени 5 по модулю многочлена второй степени. Таким образом, v_3 имеет степень меньшую или равную 1. Проводя вычисления по модулю u_3, получаем

$$v_3 = s_3(f_1 + 3u_{10}^2f_2 + 5u_{10}^4 - 4u_{10}^3f_4 - 2u_{10}f_2)x +$$

$$+ (v_{10}^2 + 4u_{10}^5 + f_0 - u_{10}^2f_2 - 3u_{10}^4f_4 + 2u_{10}^3f_3)s_3.$$

Аналогично проанализированы следующие случаи.

1.3. $u_1 \ne u_2$, $u_1 = x + u_{10}$, $u_2 = x + u_{20}$, $v_1 = v_{10}$, $v_2 = v_{20}$. Общее число операций в этом случае равно $I + 4M$.

2. $\deg(u_1) = 1$, $\deg(u_2) = 2$, $\deg(v_1) = 0$, $\deg(v_2) = 1$. Общее число операций в этом случае равно $I + 10M + 2S$.

3. $\deg(u_1) = \deg(u_2) = 2$, $\deg(v_1) = \deg(v_2) = 1$. Общее число операций в этом случае равно $I + 23M + 2S$.

Идея ускорения алгоритма Миллера заключается в том, что в его итерациях вместо преобразования дивизоров $T_1 = 2T + D_1$ предлагается выполнять преобразование $T_1 = T + (T + D_1)$. При вычислении в аффинных координатах затраты на групповую операцию удвоения больше затрат на групповую операцию сложения, как показано в таблице 2.

Таблица 2

Анализ числа операций

Метод	Первый шаг	Второй шаг	Затраты на первый шаг	Затраты на второй шаг	Общее число операций
Обычный	$T_1 = 2T$	$T_2 = T_1 + D$	$I + 22M + 5S$	$I + 22M + 3S$	$2I + 44M + 8S$
Новый	$T_1 = T + D$	$T_2 = T + T_1$	$I + 22M + 3S$	$I + 22M + 3S$	$2I + 44M + 6S$

Применим данный метод для вычисления произведения $[n]D$.

Подсчитаем количество операций S_1 для обычного метода и S_2 для нового. Заметим, что при классическом методе удвоение происходит на каждой итерации, то есть $\log_2 n$ раз, сложение — в половине случаев $\frac{\log_2 n}{2}$. В модифицированном случае необходимо $\frac{\log_2 n}{2}$ раз выполнить удвоение и столько же раз последовательно выполнить два сложения. Тогда количество операций при умножении nD_1 равно

$$S_1 = \log_2 n \cdot (I + 22M + 5S) + \frac{\log_2 n}{2} \cdot (I + 22M + 3S) =$$

$$= \log_2 n \cdot \left(\frac{3}{2} I + 33M + 6\frac{1}{2} S\right),$$

$$S_2 = \frac{\log_2 n}{2} \cdot (I + 22M + 5S) + \frac{\log_2 n}{2} \cdot (2 \cdot (I + 22M + 3S)) =$$

$$= \log_2 n \cdot \left(\frac{3}{2} I + 33M + 5\frac{1}{2} S\right).$$

Таким образом, при использовании модифицированного метода экономится $S_1 - S_2 = \log_2 n \cdot S$ операций.

Применим те же вычисления для нахождения спаривания. Нетрудно показать, что значение функции Миллера в алгоритме Миллера не зависит от представления промежуточного слагаемого $2T + D_1$. Модифицированный алгоритм тогда имеет следующий вид.

Вход: $\overline{D}_1 \in J_C(\mathbf{F}_{q^k})[n]$, $\overline{D}_2 \in J_C(\mathbf{F}_{q^k})$ с представителями D_1 и D_2 соответственно, $\mathrm{supp}(D_1) \cup \mathrm{supp}(D_2) = \varnothing$, $n = \sum_{j=0}^{s} n_i 2^i$.

Выход: $\langle D_1, D_2 \rangle_n^{\frac{q^k-1}{n}}$.

1. $f \leftarrow 1$, $T \leftarrow D_1$.
2. for $i \leftarrow s - 1$ down to 0 do
3. if $n_i = 0$ then
4. Вычисляем T', $G_{T,T}(x, y)$: $T' = 2T - \mathrm{div}(G_{T,T})$.
5. $f \leftarrow f^2 \cdot G_{T,T}(D_2)$.
6. $\overline{T} = 2\overline{T}$.

7. if $n_i = 1$ then

8. Вычисляем T', $G_{T,D_1}(x,y) : T' = T + D_1 - \mathrm{div}(G_{T,D_1})$.

9. $f := f^2 \cdot G_{T,D_1}(D_2)$.

10. $T' \leftarrow T + D_1$.

11. Вычисляем T'', $G_{T,T'}(x,y) : T'' = T + T' - \mathrm{div}(G_{T,T'})$.

12. $f \leftarrow f \cdot G_{T,T'}(D_2)$.

13. $T = T + T'$.

14. Возвращаем $f^{\frac{q^k-1}{n}}$.

Количество операций для классического и модифицированного алгоритмов:

$$S_1 = \log_2 n \cdot (T_D + C + D) + \frac{\log_2 n}{2} \cdot (T_A + C + D),$$

$$S_2 = \frac{\log_2 n}{2} \cdot (T_D + C + D) + \frac{\log_2 n}{2} \cdot (2(T_A + C + D)),$$

где C, D — числитель и знаменатель функции Миллера f. Количество операций для C равно $7M + 2S$, для D число операций есть $4M$.

Как для скалярного умножения, так и для спаривания Тейта при использовании нового метода экономится $S_1 - S_2 = \log_2 n \cdot S$ операций.

Для проективных координат затраты на операцию удвоения дивизора меньше, чем на композицию дивизоров, что делает бессмысленным применение вышеприведенного метода. Тем не менее количество операций в поле при вычислении спаривания можно сократить за счет иного представления порядка подгруппы.

Порядок подгруппы представляется в так называемой несмежной форме. Вес Хэмминга числа, приведенного в такой форме, минимален и составляет в среднем $1/3$ от всей битовой длины числа. Таким образом, выполнять последовательное удвоение и сложение дивизоров необходимо будет лишь в одной из каждых трех итераций, что по предварительной оценке снижает количество операций на $1/6$.

Можно показать, что функция Миллера в данном случае также корректно вычисляется. Шаги с 1 по 8 алгоритма Миллера совпадают с соответствующими шагами модифицированного алгоритма, представленного выше. Приведем оставшиеся шаги.

9. $f := f \cdot G_{T,D_1}(D_2)$;

10. $T' \leftarrow T + D_1$;

11. if $n_i = -1$ then

12. Вычисляем T', $G_{T,-D_1}(x,y) : T' - D_1 - \mathrm{div}(G_{T,D_1})$;

13. $f := f \cdot G_{T,-D_1}(D_2)$;

14. $T' \leftarrow T + (-D_1)$;

15. Возвращаем $f^{\frac{q^k-1}{n}}$.

Для сравнительного анализа эффективности алгоритмов были проведены компьютерные эксперименты. Использовался процессор Intel Pentium Dual CPU E2200 2.20 GHz. Результаты представлены в таблице 3.

Таблица 3

Время выполнения операций для основной кривой

Битовая длина q	Умножение (M)	Возведение в квадрат (S)	Инверсия (I)	MI-коэффициент
4117	0,002974 с	0,002346 с	0,016101 с	5,41

Пример. Уравнение кривой C: $y^2 = x^5 + 1$, степень вложения 2.

Характеристика поля $\mathbf{F}_q$: 4117 — битовое простое число.

Порядок подгруппы якобиана $r = r_1 r_2$, где r_1, r_2 — простые 512-битные числа.

Было проведено 10 измерений, выбрано среднее время выполнения. Результаты представлены в таблице 4.

Таблица 4

Результаты вычисления спаривания Тейта различными методами в аффинных координатах

Метод	Количество итераций (битовая длина порядка подгруппы)	Теоретическое количество операций	Время выполнения, с
Классический	1023	$1533I + 50589M + 9709S$	51,590
Новый	1023	$1533I + 50589M + 8687S$	47,048

В результате экономится $1022 \cdot S$ операций в поле $\mathbf{F}_{q^k}$. Операция возведения в квадрат в расширении равна по затратам $4M + 2S$ операциям в поле $\mathbf{F}_q$. Общее количество сэкономленных операций по сравнению с классическим для данного примера: $4088M + 2044S$.

Общее количество операций для случайного размера n подгруппы с использованием несмежной формы для проективных координат:

$$S = \log_2 n \cdot (T_D + F) + \frac{\log_2 n}{3} \cdot (T_A + F),$$

где $T_D = 41M + 4S$ — число операций для удвоения дивизоров; $T_A = 38M + 3S$ — для сложения дивизоров; $F = 11M + S$ — для вычисления функции Миллера. Итого: $\log_2 n \cdot \left(\frac{205}{3} M + \frac{19}{3} S \right)$ операций.

Для сравнения количество операций при использовании размера подгруппы в обычном бинарном виде:

$$S = \log_2 n \cdot (T_D + F) + \frac{\log_2 n}{2} \cdot (T_A + F),$$

что дает $\log_2 n \cdot \left(\frac{153}{2} M + 7S \right)$ операций. Экономия: $\log_2 n \cdot \left(\frac{49}{6} M + \frac{2}{3} S \right)$ операций.

Данное число соответствует количеству операций, сэкономленных в поле $\mathbf{F}_{q^k}$. Одно умножение в расширении соответствует 6 M операциям в $\mathbf{F}_q$. Как было отмечено ранее, возведение в квадрат в расширении соответствует $4M + 2S$ операциям в $\mathbf{F}_q$. Тогда общее количество сэкономленных операций в $\mathbf{F}_q$ для данного примера: $52855M + 1364S$. Результаты компьютерных экспериментов представлены в таблице 5. Было также проведено 10 измерений, выбрано среднее время выполнения.

Таблица 5

Результаты вычисления спаривания Тейта различными методами в проективных координатах

Метод	Количество итераций (битовая длина порядка подгруппы)	Теоретическое количество операций	Время выполнения, с
Классический	1023	$77748M + 7161S$	22,067
С использованием несмежной формы	1023	$69905M + 6479S$	16,299

Полученная оптимизация алгоритмов используется в протоколах доверенного шифрования в облачных системах [13].

Список литературы

1. *Sakai R., Ohgishi K., Kasahara M.* Cryptosystems Based on Pairings // Proceedings of the 2000 Symposium on Cryptography and Information Security. 2000. P. 26—28.

2. *Joux A.* A One-Round Protocol for Tripartite Diffe-Hellman // Algorithmic Number Theory Symposium. Springer-Verlag, 2000. P. 385—394.

3. *Lange T.* Formulae for Arithmetic on Genus 2 Hyperelliptic Curves // Applicable Algebra in Engineering, Communication and Computing. 2005. Vol. 15, iss. 5. P. 295—328.

4. *Choie Y., Lee E.* Implementation of Tate Pairing on Hyperelliptic Curve of Genus 2 // Information Security and Cryptology. 2004. P. 97—111.

5. *H'Eigeartaigh C.O., Scott M.* Pairing Calculation on Supersingular Genus 2 Curves // Selected Areas in Cryptography. 2007. P. 302—316.

6. *Duursma I., Gaudry P., Morain F.* Speeding up the Discrete Log Computation on Curves with Automorphisms // Advances in Cryptology. 1999. P. 103—121.

7. *Gaudry P.* An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves // Advances in Cryptology. 2000. P. 19—34.

8. *Fan X., Gong G.* Efficient Explicit Formulae for Genus 2 Hyperelliptic Curves over Prime Fields and Their Implementations. LNCS 4876. Springer, 2007. P. 155—172.

9. *Koblitz N., Menezes A.* Pairing-based Cryptography at High Security Levels // Cryptography and Coding. LNCS 3796. Springer, 2005. P. 235—249.

10. *Teruya T., Saito K., Kanayama N. et al.* Constructing Symmetric Pairings over Supersingular Elliptic Curves with Embedding Degree Three // LNCS 8365. Springer, 2014. P. 97—112.

11. *Granger R., Hess F.* Ate Pairing on Hyperelliptic Curves // Advance in Cryptology. LNCS 4515. Springer, 2007. P. 430—447.

12. *Zhang F.* Twisted Ate Pairing on Hyperelliptic Curves and Applications // Cryptology ePrint Archive, Report 2008/274, 2008.

13. *Алешников С.И., Алешникова М.В., Горбачёв А.А.* Протокол доверенного шифрования на основе модифицированного алгоритма вычисления спаривания Вейля на алгебраических кривых для облачных вычислений // Информационные технологии. 2013. № 9. С. 36—39.

Об авторах

Марина Валерьевна Алешникова — ст. преп., Балтийский федеральный университет им. И. Канта, Россия.

E-mail : aleshnikova_m_v@mail.ru

Сергей Иванович Алешников — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: elliptec@mail.ru

Андрей Александрович Горбачёв — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: terjer@mail.ru

Денис Олегович Олефиренко — асп., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: denis_cooler_1@mail.ru

The authors

Marina V. Aleshnikova, Assistant Professor, I. Kant Baltic Federal University, Russia.

E-mail: aleshnikova_m_v@mail.ru

Dr Sergey I. Aleshnikov, Associate Professor, I. Kant Baltic Federal University, Russia.

E-mail: elliptec@mail.ru

Dr Andrei A. Gorbachev, Associate Professor, I. Kant Baltic Federal University, Russia.

E-mail: terjer@mail.ru

Denis O. Olefirenko, PhD Student, I. Kant Baltic Federal University, Russia.

E-mail: denis_cooler_1@mail.ru