УДК 511.6:519.7(075.8)

С. И. Алешников, М. В. Алешникова

О СПАРИВАНИЯХ НА АБЕЛЕВЫХ МНОГООБРАЗИЯХ p-РАНГА ОДИН И ИХ КРИПТОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ

Описаны и проанализированы с точки зрения вычислительной эффективности различные виды спариваний на гиперэллиптических кривых, преимущественно на кривых рода 2 и p-ранга один для криптографических приложений.

Described and analyzed in terms of computational efficiency different types of pairings on hyperelliptic curves, especially on curves of genus 2 and p-rank one for the cryptographic applications.

Вестник Балтийского федерального университета им. И. Канта. 2014. Вып. 10. С. 155 – 161.

Ключевые слова: алгебраические кривые, гиперэллиптические кривые, якобианы кривых, абелевы многообразия, p-ранг, степень вложения, билинейные спаривания, спаривание Тэйта — Лихтенбаума, спаривание Ate, скрученное спаривание Ate, спаривание Вейля.

Key words: algebraic curves, hyperelliptic curves, Jacobians of curves, abelian varieties, p-rank, embedding degree, bilinear pairings, Tate-Lichtenbaum pairing, Ate pairing, twisted Ate pairing, Weil pairing.

Введение

Будем рассматривать алгебраические кривые родов $g = 2, 3, 4$.

Мы хотим выяснить соотношение между эффективностью вычислений в якобиане кривой и, в частности, эффективностью вычисления спариваний и криптостойкостью соответствующих криптосистем [1]. Криптостойкость определяется степенью вложения якобиана в расширение основного поля. Чем выше степень вложения, тем труднее решается задача дискретного логарифмирования, тем, соответственно, более стойка криптосистема [3; 5; 7; 9].

Эллиптические кривые условно делятся на два класса: суперсингулярные, для которых сложение точек выполняется быстро, но и степень вложения мала, так что соответствующие криптосистем не могут считаться стойкими, и обыкновенные (несуперсингулярные), для которых сложение точек вычисляется медленнее, но степень вложения высока и соответствующие криптосистемы надежны. Для кривых высших родов существует промежуточный класс кривых — кривые p-ранга 1, которые, возможно, сочетают в себе оба достоинства [11; 12]. Мы хотим исследовать пригодность таких кривых для криптографии с обеих точек зрения: эффективности вычислений и стойкости [2; 10].

Известно много различных спариваний на алгебраических кривых: Вейля, Тэйта, Ate и др. [4; 6; 8; 13]. Мы хотим проанализировать пригодность различных видов спариваний для рассматриваемых криптосистем.

1. Якобианы кривых

Пусть k — поле, $K = \overline{k}$ — его алгебраическое замыкание, C — гладкая проективная абсолютно неприводимая алгебраическая кривая над k.

Множество всех дивизоров кривой C, обозначаемое $\mathrm{Div}(C)$, образует аддитивную группу относительно этого сложения. *Степенью* дивизора D называется целое число $\deg D = \sum_{P \in C} m_P$.

Множество всех дивизоров степени 0, обозначаемое $\mathrm{Div}^0(C)$, является подгруппой группы $\mathrm{Div}(C)$. *Дивизором* рациональной функции $f \in K(C)$, $f \neq 0$, (*главным дивизором*) называется

$$\mathrm{div}(f) = \sum_{P \in C} v_P(f) P ,$$

где $v_P(f)$ — порядок функции f в точке $P \in C$. Множество всех главных дивизоров $\wp$ образует подгруппу группы $\mathrm{Div}^0(C)$. Факторгруппа $\Im_C = \mathrm{Div}^0(C)/\wp$ называется *якобианом* кривой C.

Пусть $k = \mathbb{F}_q$ — конечное поле, $P = (u, v)$ — точка C и σ — автоморфизм K над k. Тогда $P^\sigma = (\sigma(u), \sigma(v))$ — также точка кривой. Говорят, что дивизор $D = \sum m_P P$ *определен над* k, если $D^\sigma = \sum m_P P^\sigma$ равен D для любого автоморфизма σ расширения K/k. Рациональная функция $f \in K(C)$ определена над k тогда и только тогда, когда ее дивизор $\mathrm{div}(f)$ определен над k. Ясно, что дивизоры, определенные над k, образуют подгруппу группы $\mathrm{Div}(C)$ всех дивизоров. Тогда множество $\mathfrak{I}_C(k)$ всех классов дивизоров в $\mathfrak{I}$, имеющих представителей, которые определены над k, является подгруппой группы $\mathfrak{I}_C$. При этом $\mathfrak{I}_C(k)$ — конечная абелева группа. Ее называют *k-рациональным якобианом* кривой C.

2. Абелевы многообразия *p*-ранга один

Проективная алгебраическая группа A называется а*белевым многообразием*. В частности, k-рациональный якобиан $\mathfrak{I}_C(k)$ алгебраической кривой C является абелевым многообразием.

Пусть A и B — абелевы многообразия над k, $\varphi: A \to B$ — морфизм над k, такой, что $\varphi(0) = 0$, является гомоморфизмом групп. Множество $\mathrm{Hom}_k(A, B)$ таких гомоморфизмов образует абелеву группу.

Пусть φ — доминантный морфизм из A в B. Для функции $f \in k(B)$ полагаем $\varphi^*(f) = f \circ \varphi$. Тем самым определен инъективный гомоморфизм $\varphi^* : k(B) \to k(A)$. Отображение $\varphi \in \mathrm{Hom}_k(A, B)$ называется *изогенией*, если $\mathrm{Im}\,\varphi = B$ и ядро $\mathrm{Ker}\,\varphi$ конечно. Гомоморфизм $\varphi \in \mathrm{Hom}_k(A, B)$ изогения тогда и только тогда, когда выполняется одно из эквивалентных условий:

- $\dim A = \dim B$ и $\dim(\mathrm{Ker}\varphi)^0 = 0$, где $(\mathrm{Ker}\varphi)^0$ — максимальное абсолютно неприводимое подмногообразие, содержащее 0;
- φ доминантен и $k(A)/\varphi^*(k(B))$ — конечное алгебраическое расширение, *степень* изогении $\varphi : A \to B$ — число $\deg\varphi = [k(A) : \varphi^*(k(B))]$.

Пусть A — абелево многообразие над k, $n \in \mathbb{Z}$. Степень изогении $[n]$ равна $n^{2\dim A}$. Если $n = p^s$, где $p = \mathrm{char}\,k$, то $A[p^s] = \mathbb{Z}/p^{ts}\mathbb{Z}$, где $t \leqslant \dim A$ и не зависит от s. Абелево многообразие A называется *обыкновенным*, если $A[p^s] = \mathbb{Z}/p^{ts}\mathbb{Z}$, где $t = \dim A$. Говорят, что абелево многообразие A имеет *p-ранг t*, если $A[p^s] = \mathbb{Z}/p^{ts}\mathbb{Z}$.

Если E — эллиптическая кривая, то есть абелево многообразие размерности 1 и его p-ранг равен 0, то говорят, что кривая E *суперсингулярна*. Известно, что абелево многообразие A *суперсингулярно*, если оно изогенно произведению суперсингулярных эллиптических кривых. В этом случае оно имеет p-ранг 0.

3. Спаривания на гиперэллиптических кривых

Гиперэллиптическая кривая C рода $g \geqslant 1$ над $\mathbb{F}_q$ есть несингулярная плоская кривая, определяемая аффинным уравнением $y^2 + h(x)y = f(x)$, где $f(x)$ — унитарный многочлен степени $2g + 1$; $h(x)$ — многочлен степени, непревосходящей g. Зафиксируем подгруппу некоторого порядка r группы $\mathfrak{I}_C(\mathbb{F}_q)$. Говорят, что эта подгруппа имеет *степень вложения k*,

если порядок r делит $q^k - 1$, но не делит $q^i - 1$ для всех i: $0 < i < k$. Это влечет, что группа μ_r корней степени r из единицы содержится в $\mathbb{F}_{q^k}$, но не содержится ни в каком меньшем расширении поля $\mathbb{F}_q$.

Для криптографических приложений r должно быть большим простым, таким, что $r \mid \#\mathfrak{I}_C(\mathbb{F}_q)$ и $НОД(r, q) = 1$. Пусть $\mathcal{J}_C(\mathbb{F}_{q^k})[r]$ есть r-я группа кручения, $\mathcal{J}_C(\mathbb{F}_{q^k}) / r\mathcal{J}_C(\mathbb{F}_{q^k})$ — факторгруппа. Тогда спаривание Тэйта — Лихтенбаума

$$\langle \cdot, \cdot \rangle_r : \mathcal{J}_C(\mathbb{F}_{q^k})[r] \times \mathcal{J}_C(\mathbb{F}_{q^k}) / r\mathcal{J}_C(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^* / (\mathbb{F}_{q^k}^*)^r$$

корректно определяется так: пусть $\bar{D}_1 \in \mathcal{J}_C(\mathbb{F}_{q^k})[r]$, $\bar{D}_2 \in \mathcal{J}_C(\mathbb{F}_{q^k})$, где D_1 — дивизор, представляющий $\bar{D}_1$; D_2 — дивизор, представляющий $\bar{D}_2$, причем выполняется условие $\mathrm{supp}(D_1) \cup \mathrm{supp}(D_2) = \varnothing$. Существует рациональная функция $f_{r, D_1} \in \mathbb{F}_{q^k}(C)$, такая, что $\mathrm{div}(f_{r, D_1}) = rD_1 - [r]D_1 = rD_1$. Тогда по определению

$$\langle \bar{D}_1, \bar{D}_2 \rangle_r = f_{r, D_1}(D_2) = \prod_{P \in C(K)} f_{r, D_1}(P)^{\mathrm{ord}_P(D_2)}.$$

Это спаривание билинейно, невырожденно и определено с точностью до r-х степеней. Чтобы вычислять однозначно определенные значения, используют *редуцированное спаривание* $e(\bar{D}_1, \bar{D}_2) = \langle \bar{D}_1, \bar{D}_2 \rangle_r^{(q^k - 1)/r} \in \mu_r \subset \mathbb{F}_{q^k}^*$.

Главная проблема вычисления $\langle \bar{D}_1, \bar{D}_2 \rangle_r$ — построение рациональной функции f_{r, D_1} и ее значения $f_{r, D_1}(D_2)$, где $\mathrm{div}(f_{r, D_1}) = rD_1$. Миллер описал быстрый алгоритм вычисления $f_{r, D_1}(D_2)$ для дивизоров на эллиптических кривых. Этот алгоритм позднее был адаптирован для вычисления спаривания на гиперэллиптических кривых.

Пусть G_{iD_1, jD_1} — рациональная функция, такая, что $\mathrm{div}(G_{iD_1, jD_1}) = iD_1 + jD_1 - (iD_1 \oplus jD_1)$, где $\oplus$ — групповой закон в $\mathfrak{I}_C$ и $(iD_1 \oplus jD_1)$ — редуцированный дивизор. Алгоритм Миллера для гиперэллиптических кривых строит рациональную функцию f_{r, D_1} на основе следующей рекуррентной формулы:

$$f_{i+j, D_1} = f_{i, D_1} f_{j, D_1} G_{iD_1, jD_1}.$$

Опишем спаривание *Ate* на обыкновенной гиперэллиптической кривой. Пусть π — отображение Фробениуса степени q на кривой C и эндоморфизм Фробениуса якобиана $\mathfrak{I}_C$, C — гиперэллиптическая кривая над $\mathbb{F}_q$; r — большое простое число; $r \mid \#\mathfrak{I}_C(\mathbb{F}_q)$; $\mathbb{G}_1 = \mathfrak{I}_C[r] \cup \mathrm{Ker}(\pi - [1])$ и $\mathbb{G}_2 = \mathfrak{I}_C[r] \cup \mathrm{Ker}(\pi - [q])$. Тогда отображение $a(\cdot, \cdot) : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r$, $(\bar{D}_2, \bar{D}_1) \mapsto f_{q, D_2}(D_1)$, где $D_2 = \rho(\bar{D})$ — единственный редуцированный дивизор в $\bar{D}$, $D_1 \in \bar{D}_1$ и $\mathrm{supp}(D_1) \cup \mathrm{supp}(D_2) = \varnothing$, определяет невырожденное билинейное спаривание, называемое *гиперэллиптическим спариванием Ate*. Наиболее важным свойством спаривания *ate* является то, что для него не нужно заключительное возведение в степень.

Рассмотрим кручение гиперэллиптических кривых. Пусть C — кривая рода g, определенная над полем k. Кривая C' над k, изоморфная C, называется *кручением* C. Более того, кривая C' называется *кручением степени* d кривой C, если существует изоморфизм $\phi: C' \to C$, определенный над k_d, где k_d — расширение k степени d и d минимально. Для всякой кривой C, определенной над k, множество ее кручений Twist(C / k) есть множество кривых C' / k, изоморфных C над k.

Для построения кручения данной кривой C над полем k необходимо вычислить группу автоморфизмов Aut(C) кривой C. Для гиперэллиптических кривых рода 2 над конечными полями характеристики 2, 3 и 5 возможными редуцированными группами автоморфизмов являются C_2, V_4, D_8, D_{12}, $2D_{12}$, $\tilde{S}_4$, C_{10}, где C_n — циклическая группа порядка n; V_4 — четверная группа Клейна; D_n — группа диэдра порядка n, $2D_{12}$ и $\tilde{S}_4$ есть 2-накрытия группы диэдра D_{12} и симметрической группы S_4.

Степень d кручения кривой C зависит от порядка элемента из Aut(C), то есть если C' — кручение C степени d, то группа Aut(C) должна содержать элемент порядка d. Однако если char(k) > 5, то Aut(C) всегда есть подгруппа одной из перечисленных групп. В таком случае для char(k) > 5 возможны лишь случаи d = 1, 2, 3, 4, 5, 6, 8, 10. Например, для конечного поля $\mathbb{F}_q$, где q — большое простое число и $q \equiv 1 \pmod 8$ кривая $C_1 : y^2 = x^5 + ax$ имеет группу автоморфизмов $C_8 \subset \tilde{S}_4$. Кручением C_1 степени d = 8 является кривая $C_1' : y^2 = x^5 + a\lambda x$, соответствующий изоморфизм есть $(x, y) \mapsto (\lambda^{1/4}x, \lambda^{5/8}y)$, где $\lambda \in \mathbb{F}_q$ и не является l-степенным вычетом в $\mathbb{F}_q$ для $l \in \{1, 2, 4, 8\}$.

Скрученное гиперэллиптическое спаривание Ate определяется так: пусть C — гиперэллиптическая кривая над $\mathbb{F}_q$, которая имеет кручение C' степени d, r — большое простое число, $r \mid \#\mathfrak{I}_C(\mathbb{F}_q)$, k — степень вложения кривой, $m = НОД(k, d)$, $e = k / m$, ξ_m — примитивный корень степени m из единицы в $\mathbb{F}_{q^e}$. Имеем $\mathbb{G}_2 = \mathfrak{I}_C[r] \cup \mathrm{Ker}([\xi_m]\pi^e - 1)$. Тогда равенство

$$t(\overline{D}_1, \overline{D}_2) = f_{q^e,\, D_1}(D_2),$$

где $D_1 \in \overline{D}_1$, $D_2 = \rho(\overline{D}_2)$ и $\mathrm{supp}(D_1) \cup \mathrm{supp}(D_2) = \varnothing$, определяет невырожденное билинейное спаривание, называемое гиперэллиптическим скрученным спариванием *Ate*.

Гиперэллиптическое спаривание *Ate* и скрученное спаривание *Ate* допускают обобщения. Во-первых, выражения

$$f_{q \pmod r,\, D_2}(D_1)^{(q^k-1)/r} \quad \text{и} \quad f_{q^e \pmod r,\, D_1}(D_2)^{(q^k-1)/r}$$

задают спаривания, называемые *оптимизированным гиперэллиптическим спариванием Ate* и *оптимизированным скрученным спариванием Ate* соответственно. Во-вторых, выражения

$$f_{q^i \pmod r,\, D_2}(D_1)^{(q^k-1)/r} \quad \text{и} \quad f_{q^{ei} \pmod r,\, D_1}(D_2)^{(q^k-1)/r}$$

задают спаривания, называемые *обобщенным гиперэллиптическим спариванием Ate* и *обобщенным скрученным спариванием Ate* соответственно. И то и другое спаривание не нуждаются в финальном возведении в степень для получения однозначного результата спаривания.

Спаривание Вейля есть невырожденное билинейное отображение

$$e_w(\cdot,\cdot)\colon \mathcal{J}_C(\mathbb{F}_{q^k})[r]\times\mathcal{J}_C(\mathbb{F}_{q^k})[r] \to \mu_r, \text{ где } e_w(\bar{D}_1,\bar{D}_2) = (-1)^r \frac{f_{r,D_1}(D_2)}{f_{r,D_2}(D_1)}.$$

Это спаривание также не требует заключительного возведения в степень, однако нуждается в двух итерациях цикла Миллера. Для q^{ej} положим $q^{(ej)a} - 1 = Lr$, r^2 не делит $q^{(ej)a} - 1$. Пусть $q_r^{ej} \equiv q^{ej} \pmod r$. Тогда

$$\frac{f_{q_r^{ej},D_1}(D_2)}{f_{q_r^{ej},D_2}(D_1)} = e_w(\bar{D}_1,\bar{D}_2)^c,$$

где $c \equiv L(aq^{(ej)(a^{-1})})^{-1} - l \pmod r$, есть невырожденное билинейное спаривание, называние *скрученным спариванием Вейля*.

Разработаны алгоритмы вычисления спариваний и получены оценки эффективности этих алгоритмов.

Список литературы

1. *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 (205). С. 36—39.

2. *Barreto P. S. L. M., Galbraith S. et al.* Efficient pairing computation on supersingular Abelian varieties // Designs, Codes and Cryptography, 2007. Vol. 42(3).

3. *Freeman D., Stevenhagen D., Streng M.* Abelian varieties with prescribed embedding degree //ANTS. 2008. Vol. 5011. P. 60—73.

4. *Galbraith S. D., Hess F., Vercauteren F.* Hyperelliptic pairing // Pairing 2007. LNCS 4575. 2007. P. 108—131.

5. *Galbraith S. D., McKee J. F., Valenca P. C.* Ordinary Abelian varieties having small embedding degree // J. Finite Fields and Their Applications. 2007. 13. P. 800—814.

6. *Granger R., Hess F. et al.* Ate pairing on hyperelliptic curves // Advance in Cryptology–EUROCRYPT'2007. LNCS 4515. 2007. P. 430—447.

7. *Granger R., Page D., Smart N. P.* High security pairing-based cryptography revisited. Cryptology ePrint Archive. Report 2006/059. 2006.

8. *Hess F., Smart N. P., Vercauteren F.* The Ate pairing revisited // IEEE Transactions on Information Theory. 2006. Vol. 52. P. 4595—4602.

9. *Koblitz N., Menezes A.* Pairing-based cryptography at high seccurity levels // Cryptography and Coding. LNCS 3796. 2005. P. 235—249.

10. *Matsuda S., Kanayama N., Hess F. et al.* Optimized version of the Ate and twisted Ate pairing // The 11th Int. Conf. on Cryptography and Coding. LNCS 4887. 2007. P. 302—312.

11. *O'Connor L. H., McGuire G., Naehrig M. et al.* A CM construction for curves of genus 2 with p-rank 1. arXiv:0811.3434v3 [math.AG] 11 May 2010.

12. *Oort F.* Abelian varieties over finite fields // Higher-dimensional varieties over finite fields. Summer school in Göttingen. 2007.

13. *Zhang F.* Twisted Ate pairing on hyperelliptic curves and applications. Cryptology ePrint Archive, Report 2008/274, 2008.

Об авторах

Сергей Иванович Алешников — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Калининград.
E-mail: elliptec@mail.ru

Марина Валерьевна Алешникова — ст. преп., Балтийский федеральный университет им. И. Канта, Калининград.
E-mail: aleshnikova_m_v@mail.ru

About the authors

Sergey Aleshnikov — Ass. Prof., I. Kant Baltic Federal University, Kaliningrad.
E-mail: elliptec@mail.ru

Marina Aleshnikova — high instructor, I. Kant Baltic Federal University, Kaliningrad.
E-mail: aleshnikova_m_v@mail.ru