УДК 681.3.06

АЛГОРИТМ ВЫБОРА ЯКОБИАНОВ ДЛЯ НЕСИММЕТРИЧНЫХ КРИПТОСИСТЕМ

А.А. Смирнов
(представил д.т.н., проф. Ю.В. Стасев)

В статье предлагается алгоритм выбора якобианов гиперэллиптических кривых над конечным полем. Формулируются рекомендации по выбору якобианов для криптосистем на эллиптических кривых.

Формулировка проблемы. Для обеспечения безопасности информации, защиты от несанкционированного доступа и реализации процедур целостности и достоверности применяются криптосистемы, основанные на преобразованиях в группе точек эллиптических кривых. Стойкость этих криптосистем зависит от эффективности решения задачи нахождения дискретного логарифма на эллиптических кривых. Время решения задачи зависит от значения порядка кривой. Порядок эллиптической кривой можно найти, используя якобианы на гиперэллиптических кривых.

Анализ литературы показал, что в [1 – 7] проведены исследования по использованию якобианов гиперэллиптических кривых, определенных над конечным полем. В [8] проведены исследования по применению гиперэллиптических кривых в криптографии.

Целью статьи является разработка алгоритма выбора якобианов, порядок которых обеспечит требуемую стойкость криптопреобразований относительно решения задачи дискретного логарифма.

Основной материал. Для положительного целого числа g рассмотрим гиперэллиптическую кривую вида $v^2 + v = u^{2g+1}$, определенную над полем F_p из p элементов, где p – простое число, которое не делит $2g+1$. Пусть $K = F_{p^n}$. K-дивизор – конечная формальная сумма $D = \sum m_i p_i$, из $\overline{K}$ точек на кривой, которая определена любым $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Его степень равна $\sum m_i$. Конечная абелева группа из K-точек якобиана обозначается $J(K)$, это частное группы K-дивизоров степени ноль подгруппы дивизоров рациональных функций (определенных над K) на кривой. Каждый элемент $D \in J(K)$ уникально связан с парой функций $a, b \in K[u]$,

для которых $\deg a \le g$, $\deg b \le \deg a$ и $b(u)^2 + b(u) - u^{2g+1}$ являются делимыми $a(u)$; а именно, D – класс эквивалентности НОД дивизоров функций $a(u)$ и $b(u) - v$. Элемент $D \in J(K)$ тогда обозначается $\mathrm{div}(a,b)$ [1, 2].

Сложение двух элементов $\mathrm{div}(a_1, b_1)$, $\mathrm{div}(a_2, b_2) \in J(K)$, происходит следующим образом. Определим $d = d(u)$ как НОД трех полиномов $a_1(u)$, $a_2(u)$ и $b_1(u) + b_2(u) + 1$. Выберем полиномы $s_1(u)$, $s_2(u)$, $s_3(u)$ так, что $d = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + 1)$. Определим a и b:

$$a = \frac{a_1 a_2}{d^2}; \tag{1}$$

$$b(u) = \frac{s_1(u)a_1(u)b_2(u) + s_2(u)a_2(u)b_1(u) + s_3(u)(b_1(u)b_2(u) + u^{2g+1})}{d(u)} \bmod a(u). \tag{2}$$

Если $\deg a > g$, заменим пару (a,b) эквивалентной парой (a',b'):

$$a'(u) = \frac{u^{2g+1} - b(u)^2 - b(u)}{a(u)}; \tag{3}$$

$$b'(u) = -b(u) - 1 (\mathrm{mod}(a'(u)). \tag{4}$$

Для $\deg a' < \deg a$, последовательное применение этой процедуры ведет к паре (a'', b'') с $\deg a'' \le g$ такой, что $\mathrm{div}(a'', b'') = \mathrm{div}(a_1, b_1) + \mathrm{div}(a_2, b_2)$. Это и является описанием закона группы $J(K)$.

Пусть g – положительное целое число. Пусть $J(K)$ обозначает K-точки якобиана кривой $v^2 + v = u^{2g+1}$, определенной над F_p. Пусть $d = 2g+1$ взаимно простое с p, и пусть N_n обозначим $\#J(F_{p^n})$. Тогда зета-полином задается следующим образом [1]:

$$Z(T) = \prod_{j=1}^{g} (T - a_j)(T - \bar{a}_j), \tag{5}$$

на кривой $v^2 + v = u^{2g+1}$.

Он связан с N_n следующим образом:

$$N_n = \prod_{j=1}^{g} \left| 1 - a_j^n \right|^2. \tag{6}$$

Полином $Z(T)$ вычислен из числа решений $v^2 + v = u^{2g+1}$ в поле F_{p^n} для $n = 1, 2, \ldots, g$ [3].

Для упрощения вычислений введем ряд предположений. Пусть степень $d = 2g+1$ простая; f обозначает мультипликативный порядок p по модулю d так, что $d \mid p^f - 1$; $h = \frac{2g}{f}$; x – фиксированный характер над $F_{p^f}^*$ порядка d, т.е. $\chi(\rho) = e^{\frac{2\pi i}{d}}$ для некоторого генератора ρ над $F_{p^f}^*$; m_j, $1 \le j \le h$, задает набор представлений $(Z/dZ)^*$ по модулю подгрупп $\{p, p^2, \ldots, p^f\}$; χ_j обозначает характер χ^{m_j}; J_j обозначает сумму Якоби для $j = 1, 2, \ldots, h$:

$$J_j = \sum_{x \in F_{p^f}} \chi_j(x)\chi_j(1-x). \qquad (7)$$

Тогда J_j – сложное число с абсолютным значением $p^{\frac{f}{2}}$ и

$$Z(T) = \prod_{j=1}^{h} \left(T^f + J_j\right). \qquad (8)$$

Предположим, что n является взаимно простым с f, тогда

$$N_n = \prod_{j=1}^{h} \left(1 + (-1)^{n+1} J_j^n\right). \qquad (9)$$

Для криптографических систем необходимо выбрать g и n так, чтобы N_n было "почти простым" [1]. Для простого числа n это означает что $\frac{N_n}{N_1} = \prod_{j=1}^{g} \left|\frac{1-\alpha_j^n}{1-\alpha_j}\right|^2$ – простое. Это возможно только тогда, когда n взаимно простое с f. $Z_g(T)$ не должно иметь сомножителей среди рациональных чисел. Следующее утверждение описывает классы g, которые необходимо избегать, а также класс g, для которого $Z_g(T)$ является неприводимым.

Пусть $g > 1$ – целое число. Тогда отметим следующее.

1. Полином $Z_g(T)$ имеет сомножители среди рациональных чисел в случаях:

1.1) если $d = 2g+1$ – сложное число;

1.2) если $d = 2g+1$ – простое число;

1.3) если p – квадратичный невычет по модулю d,

иначе p имеет порядок g по модулю d, и тогда g – четное.

2. Полином $Z_g(T)$ имеет сомножители среди рациональных чисел в случае, если $d = 2g+1$ простое число, g – нечетное, и p имеет порядок g по модулю d.

Таким образом, для $p = 2$ и $g < 100$, полином $Z_g(T)$ неприводим по Q для g = 1, 3, 11, 15, 23, 35, 39, 51, 83, 95, 99, и приводим по Q для всех других случаев, кроме, возможно g = 36, 44, 56, 63, 75. Следовательно, для нахождения почти простого $\#J(F_{p^n})$, необходимо выбрать g так, чтобы не попадать на случаи (1.1) или (1.2) и выбрать значение n взаимно простым с f. Для $p = 2$ определим первые значения g с неприводимыми $Z_g(T)$:

$$Z_1(T) = T^2 + 2;$$

$$Z_3(T) = T^6 - 2T^3 + 8;$$

$$Z_{11}(T) = T^{22} - 48T^{11} + 2048;$$

$$Z_{15}(T) = T^{30} - 6T^{25} - 16T^{20} + 325T^{10} - 6144T^5 + 32768.$$

С учетом проведенных исследований определим алгоритм выбора подходящих якобианов для несимметричных криптосистем.

1. Если J – якобиан $v^2 + v = u^d$ с простым $d = 2g+1$, то нетрудно показать что $d \mid \#J(F_p)$. Это предотвращает такое условие, что $\#J(F_p)$ непростой для всех очень маленьких значений p и d (с $\#J(F_p) \sim p^g$). Однако, $\#J(F_p) \sim \frac{p^g}{d}$ может быть простым. Например, для $g = 15$, $d = 31$, $p = 2$ имеем $\#J(F_2) = Z_{15}(1) = 31 \cdot 853$.

2. Для фиксированного простого p описание закона группы $J(K)$ дает нам источник якобианов над F_p с неприводимым $Z_g(T)$. Для кривых вида $v^2 + v = u^d$, – $d \equiv 3 (\mathrm{mod}\, 4)$ является простым числом, для которого p – квадрат примитивного корня по модулю d. Для заданного p, частота, с которой такое d, встречается рассчитана Е. Артином [4], согласно которому, существует постоянная положительная вероятность того, что для простого $d \equiv 3 (\mathrm{mod}\, 4)$ существует p как квадрат примитивного корня. Например, когда $p = 2$ (когда $d \equiv 7 (\mathrm{mod}\, 8)$, с числа 2 должен начинаться квадратичный остаток по модулю d), число $d < x$ имеет асимптотическое значение приближаю-

щееся к $c\frac{x}{4\log x}$, где $c = \prod_{\text{простые} \geq 3}\left(1-\frac{1}{l(l-1)}\right) \approx 0.746\ldots$.

3. Существует несколько подходов для нахождения подходящего якобиана кривых над конечным полем F_{p^n}:

(3, а) Можно фиксировать род g и поле (то есть p и n), и изменять коэффициенты уравнения кривой. Поскольку эти коэффициенты изменяются, то число точек на якобиане будет почти однородно распределено в интервале формы $\left(p^{gn} - cp^{\left(g-\frac{1}{2}\right)n}, p^{gn} + cp^{\left(g-\frac{1}{2}\right)n}\right)$. Данный подход был изучен подробно, когда p – большое число, для случаев: $g=1$, $n=1$ [5] и $g=2$, $n=1$ [1].

(3, б) Можно определять кривую с рациональными коэффициентами, и рассматривать якобиан с редукцией по модулю p (т.е. над полем F_p), изменяя p. В случае $g=1$ формулы вероятности того, что соответствующая эллиптическая кривая имеет простой порядок, приведены в [6].

(3, в) Можно фиксировать F_p (или конечное расширение F_p) и определять кривую с коэффициентами в этом поле. Тогда рассмотрим $J(F_{p^n})$, т.е. группу точек J с координатами в конечном расширении поля определения, которое выбрано так, чтобы $\#J\left(F_{p^n}\right)$ был "почти простым" [1]. Для этого кривая должна быть выбрана так, чтобы ее зета-полином $Z(T) = \prod_{j=1}^{2g}(T-\alpha_j)$ был неприводимым по Q, то есть все α_j были сопряжены с $\alpha = \alpha_1$. Предположим, что кривая определена над полем F_p и имеет неприводимый зета-полином. Рассмотрим все расширения F_{p^n} простой степени n. В этом случае интересна простота нормы алгебраического целого числа $\frac{\alpha^n - 1}{\alpha - 1}$, поскольку n изменяется. Это обобщение простой проблемы Марсенна, и наиболее вероятная частота возникновения простых значений предсказана эвристической оценкой той же самой формы, как в классическом случае Марсенна [7].

(3, г) Можно фиксировать поле F_{p^n} и исследовать семейство кривых изменяющегося рода. Если p^n – малое, размер группы точек будет расти быстро с родом, так как он имеет порядок p^{gn}. Если существует такое требование, что #J должен быть простым числом или произведением

большого простого и маленького сомножителя, то необходимое условие состоит в том, что зета-полином должен быть неприводимым.

Преимущество подхода (3, г) состоит в дополнении еще одного параметра для изменения (род g), состоящего в том, что можно ограничивать себя кривыми со специальными свойствами симметрии. Это дает возможность вычислить число точек гораздо быстрее, чем в случае общей кривой (также несколько быстрее выполняется алгоритм обнаружения мультипликативных точек).

Вывод. Так как алгоритмы вычисления индекса исчисления для нахождения дискретных логарифмов над $F^*_{p^n}$ неприменимы на эллиптических или гиперэллиптических кривых [8], то единственный известный алгоритм для нахождения дискретного логарифма в $J\left(F_{p^n}\right)$ требует времени пропорционально времени вычисления квадратного корня самого большого простого сомножителя в $\#J\left(F_{p^n}\right)$. Таким образом, для криптосистем, основанных на проблеме решения дискретного логарифма, использование $J\left(F_{p^n}\right)$ безопасно при относительно маленьком p^n (даже когда $p = 2$). С точки зрения выполнения, эта особенность может компенсировать время, которое добавляется при вычислении более сложного действия группы.

ЛИТЕРАТУРА

1. *Koblitz N. Hyperelliptic cryptosystems. – http://www.crypto.koblitz.org*
2. *Cantor D. Computing in the jacobian of a hyperelliptic curve // Math of Computation. – 1987. – 48. – P. 95 – 101.*
3. *Weil A. Numbers of solutions of equations in finite fields // Bull. Am.tr. Math. Soc. – 1949. – 55. – P. 497 – 508.*
4. *Shanks D. Solved and Unsolved Problems in Number Theory. – N- Y., 1985. – 205 p.*
5. *Lenstra H. Factoring integers with elliptic curves. Report 86-18. – Mathematics Institute, Universities van Amsterdam, 1986. – 35 p.*
6. *Koblitz N. Primality of the number of points on an elliptic curve over a finite field // Pacific J. Math. – 1988. – 131. – P. 157 – 165.*
7. *Wagstaff S. Divisors of Mersenne Number // Math of Computation. – 1983. – 40. – P. 385 – 397.*
8. *Miller V. Use of elliptic curves in cryptography // Advance in Cryptology. Crypto '85, Springer-Verlag, New York. – 1986. – P. 417 – 426.*

Поступила 18.12.2003

***СМИРНОВ Алексей Анатольевич**, адъюнкт ХВУ. В 1999 году окончил ХВУ. Область научных интересов – защита информации в автоматизированных системах управления.*