УДК 681.3

Л. В. Гортинская, Е. С. Дернова, Д. Н. Молдовян, П. А. Молдовяну

ПОСТРОЕНИЕ КОНЕЧНЫХ ГРУПП ВЕКТОРОВ ДЛЯ СИНТЕЗА АЛГОРИТМОВ ЦИФРОВОЙ ПОДПИСИ

Рассматривается задача построения конечных коммутативных и некоммутативных групп m-размерных векторов, содержащих подгруппы простого порядка большого размера, а также построения алгоритмов цифровой подписи на их основе.

Ключевые слова: *конечные группы m-размерных векторов, электронная цифровая подпись, криптографические алгоритмы.*

Введение. Для придания юридической силы электронным документам применяется электронная цифровая подпись (ЭЦП). Алгоритмы, используемые при создании ЭЦП, основаны на вычислительно сложных задачах с применением конечных алгебраических структур с ассоциативной операцией [1, 2]. При построении схем ЭЦП наиболее часто используется задача дискретного логарифмирования (ЗДЛ) в мультипликативных группах большого простого порядка, содержащихся в конечных простых полях Галуа порядка p, $GF(p)$, или расширенных — $GF(p^m)$. При этом в качестве простого поля $GF(p)$ используется кольцо $\mathbf{Z}_p$, где p — простое число большого размера, а в качестве расширенного $GF(p^m)$ — конечные поля многочленов (m — натуральное число). Для обоих типов полей были предложены методы решения ЗДЛ, имеющие субэкспоненциальную сложность, в соответствии с ними для обеспечения достаточной стойкости алгоритмов ЭЦП требуется использовать поля $GF(p)$ и $GF(p^m)$ размером порядка 1024 бит и более, что ограничивает производительность процедур.

Более высокую производительность обеспечивают алгоритмы ЭЦП, основанные на применении конечных групп точек эллиптической кривой (ЭК), групповой операцией в которых является операция сложения (композиции) точек. Для решения ЗДЛ на эллиптической кривой известны только методы, имеющие экспоненциальную сложность, благодаря чему возможно использовать ЭК с точкой (x, y), длина x—y лежит в пределах 160—320 бит. Однако возрастание производительности в случае применения ЭК ограничено тем, что операция композиции точек в качестве составного элемента включает вычисление обратных значений в конечном поле, над которым задана ЭК [3—5].

Недавно в качестве примитивов алгоритмов ЭЦП были предложены конечные коммутативные группы и поля, формируемые в векторных пространствах, в которых определяется специальная операция умножения [6]. В этой работе показано, что при соответствующих параметрах конечное векторное пространство является конечным полем, содержащим подгруппы достаточно простого порядка, размер которого близок к размеру порядка группы. Однако вопрос формирования нециклических подгрупп векторов, содержащих подгруппы большого простого порядка, остался открытым. Также не был рассмотрен вопрос формирования некоммутативных конечных групп векторов, представляющих интерес для синтеза алгоритмов ЭЦП.

В настоящей работе рассматривается построение нециклических групп векторов, содержащих подгруппы большого простого порядка, а также некоммутативных конечных групп векторов. Интерес к конечным группам векторов обусловлен тем, что в них сложность ЗДЛ представляется более высокой, поскольку элементы задачи не могут быть представлены в виде степеней некоторого фиксированного элемента.

Определение операции умножения в конечном векторном пространстве. Конечное векторное пространство представляет собой множество элементов (векторов) вида

$a\mathbf{e} + b\mathbf{i} + \ldots + c\mathbf{j}$, где $a, b, \ldots, c$ — координаты, являющиеся элементами конечного простого поля $GF(p)$; $\mathbf{e}, \mathbf{i}, \ldots \mathbf{j}$ — базисные векторы, которые могут быть представлены также в виде набора координат $(a, b, \ldots, c)$. Операция сложения векторов может быть представлена следующей формулой:

$$(a\mathbf{e} + b\mathbf{i} + \ldots + c\mathbf{j}) + (x\mathbf{e} + y\mathbf{i} + \ldots + z\mathbf{j}) = (a + x)\mathbf{e} + (b + y)\mathbf{i} + \ldots + (c + z)\mathbf{j}.$$

В настоящей работе рассматривается задача построения мультипликативных групп векторов, различающихся видами операции умножения. Все варианты операции умножения определяются в соответствии с работой [6] по общему правилу умножения каждой компоненты первого вектора-сомножителя на каждую компоненту второго вектора-сомножителя с сохранением в общем случае порядка следования перемноженных компонент. Произведения двух базисных векторов заменяются на вектор $\gamma\mathbf{v}$, где $\gamma \in GF(p)$ и $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \ldots, \mathbf{j}\}$. Конкретному виду операции умножения свойствен конкретный вид такой подстановки. Формальное представление умножения следующее:

$$(a\mathbf{e} + b\mathbf{i} + \ldots + c\mathbf{j})\,(x\mathbf{e} + y\mathbf{i} + \ldots + z\mathbf{j}) = ax\mathbf{ee} + ay\mathbf{ei} + \ldots$$
$$+ az\mathbf{ej} + \ldots + bx\mathbf{ie} + by\mathbf{ii} + \ldots + bz\mathbf{ij} + \ldots + cx\mathbf{je} + cy\mathbf{ji} + \ldots + cz\mathbf{jj},$$

где каждое из произведений **ee**, **ei**, **ej**, **ie**, **ii**, …, **ij**, …, **je**, **ji**, …, **jj** следует заменить на значение $\gamma\mathbf{v}$, задаваемое таблицей умножения базисных векторов (ТУБВ). Конкретный вариант этой таблицы определяется конкретным вариантом операции умножения m-мерных векторов. После выполнения указанной подстановки получается некоторая сумма однокомпонентных векторов. Синтез ТУБВ выполняется таким образом, чтобы операция умножения векторов была ассоциативной и коммутативной для формирования коммутативных групп векторов или некоммутативной — для формирования некоммутативных групп векторов.

Таблицы умножения базисных векторов. В данной работе рассматривается построение мультипликативных групп в векторном пространстве, заданном не над $\mathbf{Z}_p$, а над конечным кольцом $\mathbf{Z}_n$, где $n = kp$, k — простое число. При этом операции сложения и умножения координат векторов и коэффициентов растяжения, фигурирующие в определении операции умножения векторов, рассматриваются в кольце $\mathbf{Z}_n$.

Для случаев $m = 5$ и 7 правила умножения базисных векторов могут быть заданы табл. 1 и 2. Данные ТУБВ определяют для произвольных комбинаций значений коэффициентов растяжения $\varepsilon, \mu, \tau, \lambda \in \mathbf{Z}_n$ операцию умножения, обладающую свойствами ассоциативности и коммутативности.

Таблица 1

Операция умножения	**e**	**i**	**j**	**k**	**u**
e	**e**	**i**	**j**	**k**	**u**
i	**i**	ε**λj**	ε**μk**	ε**λu**	ε**μτλe**
j	**j**	ε**μk**	ε**μu**	ε**μτλe**	**μτi**
k	**k**	ε**λu**	ε**μτλe**	**τλi**	**τλj**
u	**u**	ε**μτλe**	**μτi**	**τλj**	**μτk**

Таблица 2

Операция умножения	**e**	**i**	**j**	**k**	**u**	**v**	**w**
e	**e**	**i**	**j**	**k**	**u**	**v**	**w**
i	**i**	**λεj**	**λεk**	**τεu**	**λεv**	**λεw**	**τλεμe**
j	**j**	**λεk**	**τεu**	**τεv**	**λεw**	**τλεμe**	**τμk**
k	**k**	**τεu**	**τεv**	**τεw**	**τλεμe**	**τμi**	**τμj**
u	**u**	**λεv**	**λεw**	**τλεμe**	**λμv**	**λμj**	**λμk**
v	**v**	**λεw**	**τλεμe**	**τμi**	**λμj**	**λμk**	**τμu**
w	**w**	**τλεμτe**	**τμk**	**τμj**	**λμk**	**τμu**	**τμv**

Синтез коммутативных групп, содержащих подгруппы с большим размером простого порядка. Рассмотрим подмножество $\{\mathbf{Z}\}$ m-мерных ненулевых векторов, координаты которых являются элементами кольца $\mathbf{Z}_n$, где $n = kp$, $p >> k$, причем значение коэффициента при базисном векторе не делится на k, $\mu=\tau-\lambda=1$, число k делит число ε. Операцию умножения векторов зададим по общей схеме с использованием табл. 1, 2. Легко видеть, что такая операция умножения, выполняемая над двумя векторами из рассматриваемого подмножества, дает в результате вектор, принадлежащий этому же множеству. Мощность рассматриваемого подмножества равна

$$\#\{\mathbf{Z}\} = p(k-1)(kp)^{m-1},$$

где $p(k-1)$ — число возможных значений первой координаты, а $(kp)^{m-1}$ — число возможных комбинаций значений остальных координат. Совокупность всех векторов $\mathbf{Z}$, для которых существует обратный вектор $\mathbf{Z}^{-1}$, будет образовывать группу, порядок которой равен

$$\Omega = \#\{\mathbf{Z}\} - \#\{\mathbf{N}\},$$

где $\{\mathbf{N}\}$ — совокупность всех векторов, принадлежащих подмножеству $\{\mathbf{Z}\}$, для которых не существует обратных значений. Определим мощность $\{\mathbf{N}\}$. Векторы, для которых нет обратных значений, имеют следующий вид:

$$\mathbf{N} = (q_1 p, q_2 p, \ldots, q_m p),$$

где $q_1 \in \{1, 2, \ldots, k-1\}$ и $q_2, q_3, \ldots, q_m \in \{0, 1, 2, \ldots, k-1\}$ (нулевой вектор не входит в подмножество $\{\mathbf{Z}\}$). Легко показать, что для таких векторов отсутствуют обратные значения. Действительно, из определенной операции умножения непосредственно вытекает, что у вектора $\mathbf{V} = \mathbf{NX}$ для произвольного вектора $\mathbf{X}$ каждая из координат делится на p, следовательно, $\mathbf{V}$ не может быть единичным вектором $(1, 0, 0, \ldots, 0)$. Число векторов $\mathbf{N}$ равно $\#\{\mathbf{N}\} = (k-1)k^{m-1}$, следовательно, порядок рассматриваемой группы векторов не превышает

$$\Omega = p(k-1)(kp)^{m-1} - (k-1)k^{m-1} = (k-1)k^{m-1}(p^m - 1).$$

Это значение достигается, если m делит $p-1$, а ε является невычетом степени m по модулю p. Покажем, что это действительно так. Рассмотрим некоторый вектор $\mathbf{Z} = (a, b, ..., c)$, принадлежащий множеству $\{\mathbf{Z}\}$. Перейдем от вектора $\mathbf{Z}$ к вектору $\mathbf{Z}' = (a', b', ..., c')$, где $a' = a \bmod p$, $b' = b \bmod p$, ..., $c' = c \bmod p$. Вектор $\mathbf{Z}'$ принадлежит при заданных условиях к векторному полю $GF(p^m)$ [6]. Поскольку $\mathbf{Z}' \neq (0, 0, \ldots, 0)$, то в векторном поле $GF(p^m)$ относительно неизвестного вектора $\mathbf{X}'$ существует решение уравнения $\mathbf{Z}'\mathbf{X}' = \mathbf{E}$, где $\mathbf{E} = (1,0,\ldots,0)$. Координаты вектора $\mathbf{X}' = (x', y', .., z')$ удовлетворяют системе сравнений следующего вида:

$$\left.\begin{aligned} f_{11}(a',b',...,c')x' + f_{12}(a',b',...,c')y' + ... + f_{1m}(a',b',...,c')z' &= 1,\\ f_{21}(a',b',...,c')x' + f_{22}(a',b',...,c')y' + ... + f_{2m}(a',b',...,c')z' &= 0,\\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot&\\ f_{m1}(a',b',...,c')x' + f_{m2}(a',b',...,c')y' + ... + f_{mm}(a',b',...,c')z' &= 0. \end{aligned}\right\}$$

В данной системе коэффициенты f_{tl} при неизвестных x', y', ..., z' определяются коэффициентами растяжения и координатами вектора $\mathbf{Z}'$. Известно, что если обе части сравнения и модуль делятся на одно и то же целое число, то обе части сравнения и модуль можно разделить на это число, получив в результате эквивалентное сравнение (см. [7], теорема 128). Заменив в этой системе сравнений a' на a, b' на b, ..., c' на c и умножив левую и правую части каждого сравнения и модуль на число t, получим систему сравнений, эквивалентную исходной. В векторном множестве $\{\mathbf{Z}\}$ полученной системе соответствует векторное уравнение $\mathbf{ZX} = \mathbf{E}'$, где $\mathbf{E}' = (t,0,\ldots,0) = tE$. Очевидно, что вектор $\mathbf{X} = (tx', ty', .., tz') = t\mathbf{X}'$ является решением последнего уравнения, которое можно представить в виде $t\mathbf{ZX}' = t\mathbf{E}$, откуда следует $\mathbf{ZX}' = \mathbf{E}$, т.е. $\mathbf{X}'$ является вектором, обратным $\mathbf{Z}$. Таким образом, при $m \mid (p-1)$ и ε, являющемся невычетом степени m по модулю p, всем векторам множества $\{\mathbf{Z}\}$, кроме векторов вида $\mathbf{N}$, можно поставить в соответствие единственный обратный вектор, что и требовалось

доказать. Теоретически определенное значение $\Omega = (t-1)t^{m-1}(p^m - 1)$ подтверждается вычислительным экспериментом.

При простом значении m, таком, что $m \mid (p-1)$, значение p можно выбрать таким образом, что множитель $q = m^{-1}(p^{m-1} + p^{m-1} + \ldots + p + 1)$, содержащийся в разложении числа $p^m - 1$, будет простым. Некоторые конкретные варианты таких значений p приведены в табл. 3 (знак „\\“ обозначает перенос записи числа на другую строку). Таким образом, построенная нами группа векторов содержит подгруппу простого порядка длиной $|q|$ в двоичном представлении: $|q| = (m-1)|p| - |m| \approx (m-1)|p|$. Для построения алгоритмов ЭЦП требуется использовать подгруппы простого порядка q размером не менее $|q| \geq 160$ бит. Для этой цели следует выбрать простое число p размером $|p|$ при условии

$$|p| \geq \frac{|q| - |m|}{m-1} \approx \frac{|q|}{m-1} \quad \text{(бит)}.$$

Для синтеза алгоритмов ЭЦП удобно использовать кольца размерностью $m \in \{3, 5, 7, 11, 13, 17, 19\}$. При выборе конкретных значений m и k следует учитывать требования к производительности алгоритмов ЭЦП, вариант реализации и обеспечиваемый уровень стойкости. Для синтеза ТУБВ, соответствующих случаям $m = 3, 11, 13, 17, 19$, можно воспользоваться результатами работ [6, 8].

Таблица 3

m	p	$q = m^{-1}(p^{m-1} + p^{m-1} + \ldots + p + 1)$
5	731 347 069 147	286 084 350 321 693 088 102 651 075 474 527 140 170 997 913 161
5	50 676 921 106 512 713	6 595 396 132 044 187 165 178 914 150 733 683 078 979 644 173 924 260 \\ 305 243 710 080 341
7	186 419 693	41 971 136 855 362 349 259 612 655 092 913 923 374 434 953 935 443
11	34 919	2 695 444 645 954 794 709 894 042 480 955 311 929 186 425 401
13	8693	186 245 641 178 891 833 068 301 313 943 899 460 753 528 874 501

Построение некоммутативных групп векторов. Некоммутативные группы векторов, заданных над простым полем $GF(p)$ и имеющих размерность $m = 4$, были построены путем задания операции умножения по табл. 4. В построенных группах для произвольных ненулевых значений коэффициентов A, B и C максимальное значение порядка векторов равно $\Omega_{\max} = p(p-1)(p+1)$.

Таблица 4

Операция умножения	**e**	**i**	**j**	**k**
e	**e**	**i**	**j**	**k**
i	**i**	$-AC$**e**	A**k**	$-C$**j**
j	**j**	$-A$**k**	$-AB$**e**	B**i**
k	**k**	C**j**	$-B$**i**	$-BC$**e**

Для синтеза алгоритмов ЭЦП представляет интерес выбор простого числа p, при котором $p + 1 = 2q$, а также использование циклической подгруппы порядка q. Например, при $p = 87\,049\,239\,434\,461$, $A = 1$, $B = 2$ и $C = 3$ вектор $\mathbf{G} = (12\,051\,687\,713\,738,\ 12\,743\,450\,807\,620,\ 58\,233\,746\,685\,306,\ 75\,018\,447\,720\,758)$ имеет простой порядок $q = 43\,524\,619\,717\,231$.

Синтез алгоритмов ЭЦП на основе циклических подгрупп достаточно большого простого порядка, содержащихся в группах многомерных векторов, может быть выполнен по аналогии с алгоритмами [9, 10], построенными с учетом сложности задачи дискретного логарифмирования в конечном простом поле. Рассмотрим возможный вариант обобщенной схемы ЭЦП, предположим, что в нем используется циклическая группа векторов $\mathbf{\Gamma}$, имеющая достаточно большой порядок q ($|q| \geq 160$ бит). Например, в качестве $\mathbf{\Gamma}$ может быть использована подгруппа максимального простого порядка, содержащаяся в векторной группе, заданной над кольцом $\mathbf{Z}_n$, где $n = kp$, $k = 8693$ и $p = 50\,676\,921\,106\,512\,713$ (см. табл. 3), или под-

группа порядка q в некоммутативной группе, построенной в предыдущем разделе. При указанных параметрах кольца $\mathbf{Z}_n$ в группе векторов содержится подгруппа простого порядка, размер которой превышает 200 бит.

Подписывающий формирует свой открытый ключ $\mathbf{Y}$ в виде вектора $\mathbf{Y} = \mathbf{G}^x$, где $\mathbf{G}$ — вектор, являющийся генератором группы $\mathbf{\Gamma}$. Формирование подписи к сообщению M выполняется следующим образом:

1) выбрать случайное число $k < q$ и вычислить вектор $\mathbf{R} = \mathbf{G}^k$;

2) используя некоторую криптографически стойкую хэш-функцию F_h, вычислить хэш-код h от сообщения M с присоединенным к нему вектором $\mathbf{R}$: $h = F_h(M, \mathbf{R})$. Значение h будет первым элементом ЭЦП;

3) вычислить второй элемент ЭЦП: $s = xh + t \bmod q$.

Проверка подлинности подписи (h, s) состоит в следующем:

1) вычисляется вектор $\mathbf{R}' = Y^{q-h}\mathbf{G}^s$;

2) вычисляется значение $h' = F_h(M, \mathbf{R}')$;

3) сравниваются значения h' и h; если $h' = h$, то ЭЦП признается подлинной.

Заключение. Построены конечные коммутативные нециклические группы векторов, содержащие подгруппы простого порядка большого размера, и конечные некоммутативные группы, перспективные для применения в алгоритмах ЭЦП и открытого распределения ключей. Для случаев пяти- и семимерных векторов предложены таблицы умножения базисных векторов, содержащие четыре независимых коэффициента растяжения. Особенностью построенных коммутативных групп является то, что координаты векторов являются элементами конечного кольца $\mathbf{Z}_{kp}$. При соответствующем выборе конкретных значений p в нециклической группе содержится подгруппа простого порядка длиной $(m-1)|p| - |m|$ бит. Некоммутативная группа построена для случая четырехмерных векторов, заданных над простым конечным полем. На основе построенных групп векторов могут быть разработаны алгоритмы ЭЦП, обладающие высокой производительностью.

Для дальнейших исследований интерес представляет разработка некоммутативных групп векторов для случаев $m = 6$, 8 и 16 и синтез криптоалгоритмов с открытым ключом на основе сложности вычисления сопрягающего элемента [11] в некоммутативных конечных группах векторов.

Работа поддержана грантом РФФИ № 08-07-00096-а.

СПИСОК ЛИТЕРАТУРЫ

1. *Венбо Мао*. Современная криптография. Теория и практика. М.—СПб—Киев: Изд. дом „Вильямс“, 2005. 763 с.
2. *Шнайер Б*. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. М.: ТРИУМФ, 2002. 816 с.
3. *Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А*. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. М.: КомКнига, 2006. 324 с.
4. *Болотов А. А., Гашков С. Б., Фролов А. Б.* Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006. 274 с.
5. *Koblitz N.* A Course in Number Theory and Cryptography. Berlin: Springer-Verlag, 2003. 236 p.
6. *Молдовян Н.А.* Алгоритмы аутентификации информации в АСУ на основе структур в конечных векторных пространствах // Автоматика и телемеханика. 2008. № 12. С. 163—177.
7. *Бухштаб А. А.* Теория чисел. М.: Просвещение, 1966. 384 с.
8. *Молдовян Д. Н., Молдовяну П. А.* Задание умножения в полях векторов большой размерности // Вопросы защиты информации. 2008. № 3(82). С. 12—17.
9. *Молдовян Н. А.* Практикум по криптосистемам с открытым ключом. СПб: БХВ-Петербург, 2007. 298 с.

10. *Menezes A. J., Van Oorschot P. C., and Vanstone S. A*. Handbook of Applied Cryptography. Boca Raton, FL: CRC Press, 1997. 780 p.

11. *Ko K. H., Lee S. J., Cheon J. H., Han J. W., Kang J.-S., Park Ch.* New Public Key Cryptosystems Using Braid Groups // Advances in cryptology — CRYPTO 2000. Proc. Springer-Verlag LNCS. 2000. Vol. 1880. P. 166—183.

Сведения об авторах

Лидия Вячеславовна Гортинская — Научно-исследовательский институт „Вектор“, Санкт-Петербург; старший научный сотрудник; E-mail: lydia-gort@mail.ru

Евгения Сергеевна Дернова — аспирант; Санкт-Петербургский государственный электротехнический университет „ЛЭТИ“, кафедра автоматизированных систем обработки информации и управления; E-mail: evgeshka19@mail.ru

Дмитрий Николаевич Молдовян — Санкт-Петербургский институт информатики и автоматизации РАН; младший научный сотрудник; E-mail: mnd.spectr@mail.ru

Петр Андреевич Молдовяну — Научно-исследовательский институт „Вектор“, Санкт-Петербург; начальник службы главного метролога; E-mail: nmold@mail.ru

Рекомендована НИИ „Вектор“

Поступила в редакцию
12.10.09 г.