УДК 681.3

КОНЕЧНЫЕ ГРУППЫ С ЧЕТЫРЕХМЕРНОЙ ЦИКЛИЧНОСТЬЮ КАК ПРИМИТИВЫ ЦИФРОВОЙ ПОДПИСИ

П. А. Молдовяну,
канд. техн. наук, начальник службы главного метролога
ФГУП НИИ «Вектор»
Д. Н. Молдовян,
аспирант
Хо Нгок Зуй,
аспирант
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

Для синтеза производительных алгоритмов электронной цифровой подписи предлагается использовать вычислительно сложную задачу извлечения корня большой простой степени в конечных мультипликативных группах четырехмерных векторов, заданных над кольцом специального вида. Показано, что строение данного типа групп описывается в терминах четырехмерной цикличности. Особенности строения использованы для разработки алгоритмов нахождения корней большой простой степени в случае делимости порядка группы на квадрат степени корня. Предложена новая, более производительная схема электронной цифровой подписи.

Ключевые слова *— конечные группы, строение групп, вычислительно сложная задача, вычисление корней, цифровая подпись.*

Введение

Ранее [1, 2] были предложены конечные алгебраические структуры, заданные в конечном векторном пространстве, для построения алгоритмов электронной цифровой подписи (ЭЦП) на основе сложности задачи дискретного логарифмирования. В работе [3] показано, что в специальных частных случаях в качестве примитива алгоритмов ЭЦП перспективна задача извлечения корней большой простой степени k в конечных простых полях с характеристикой $p \geq 2^{1024}$. Одним из требований обеспечения высокой вычислительной сложности задачи нахождения корней в группах известного порядка является делимость порядка группы на k^2 при достаточно большом размере числа k, т. е. при $|k| \geq 160$ бит. Задача извлечения корней может быть решена [4] в случае циклических групп посредством предварительного вычисления дискретного логарифма от подкоренного значения. Для простых конечных полей это обстоятельство накладывает требование использовать поля с характеристикой большого размера, что ограничивает производительность алгоритмов ЭЦП.

Для повышения производительности схем ЭЦП на основе сложности извлечения корней в группах известного порядка предложено [5] использовать нециклические конечные группы двухмерных векторов. Благодаря особенностям строения конечных групп векторов в последнем случае построение стойких схем ЭЦП оказалось возможным при размере степени корня меньше 160 бит, т. е. при $|k| \geq 80$ бит. Интересно рассмотреть нециклические конечные группы многомерных векторов в качестве примитивов для схем ЭЦП, использующих сложность задачи вычисления корней. При этом с ростом размерности можно и дальше снижать размер степени корня с сохранением достаточно высокой трудности задачи извлечения корней, благодаря чему имеется потенциальная возможность повысить производительность алгоритмов ЭЦП. Однако с ростом размерности векторов в схемах ЭЦП может возникнуть потребность использовать более одного специально вычисляемого вектора в качестве открытого ключа, поскольку максимальное значение порядка при заданной общей длине вектора уменьшается. В связи с этим представляется компромиссным решением выбор размерности, равной четырем, когда при разработке алгоритмов ЭЦП можно ограничиться использованием двух векторов в качестве открытого ключа. При дальнейшем увеличении размерности векторов потре-

буется дальнейшее увеличение общего размера открытого ключа при незначительном дополнительном выигрыше в производительности.

Нециклические конечные коммутативные группы векторов, заданных над конечными полями, в общем случае имеют многомерное циклическое строение и содержат большое число циклических подгрупп одного и того же порядка [6]. Эти группы Г относятся к конечным группам известного порядка, поскольку из условий задания группы легко вычисляется значение ее порядка Ω. Обозначим через $\Omega_{\max}^{\text{цикл}}$ максимальный порядок циклических подгрупп, содержащихся в Г. С учетом особенностей строения групп векторов и результатов работ [3, 4] высокая сложность задачи извлечения корней степени k обеспечивается требованием делимости $\Omega_{\max}^{\text{цикл}}$ на k^2 и достаточно большим значением отношения $\Omega/\Omega_{\max}^{\text{цикл}}$.

В данной работе рассматривается математическая задача построения нециклических конечных групп четырехмерных векторов, удовлетворяющих отмеченным выше двум требованиям, и их применение для синтеза алгоритмов ЭЦП, основанных на сложности задачи извлечения корней большой простой степени.

Ниже используется термин многомерной цикличности в понимании работы [5], а именно, под μ-мерной цикличностью группы понимается, что ее минимальная система образующих включает μ элементов. В частности, каждый элемент системы образующих может иметь одно и то же значение порядка. Это случай однородной многомерной цикличности, который представляет особый интерес для построения алгоритмов ЭЦП.

Построение нециклических конечных групп четырехмерных векторов

Рассмотрим множество векторов вида $(a, b, c, d) = a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, где $\mathbf{e}$, $\mathbf{i}$, $\mathbf{j}$ и $\mathbf{k}$ — формальные базисные векторы; a, b, c и d — целые числа, принадлежащие конечному кольцу $\mathbb{Z}_m$, называемые координатами. Выражения $a\mathbf{e}$, $b\mathbf{i}$, $c\mathbf{j}$ и $d\mathbf{k}$ обозначают векторы $(a, 0, 0, 0)$, $(0, b, 0, 0)$, $(0, 0, c, 0)$ и $(0, 0, 0, d)$ соответственно и называются компонентами вектора (a, b, c, d). Определим операцию сложения векторов как сложение одноименных координат: $(a, b, c, d) + (x, y, z, w) = (a + x, b + y, c + z, d + w)$, где знак «+» применен для обозначения двух разных операций — сложения элементов кольца $\mathbb{Z}_m$ и сложения векторов, что не вносит неопределенности ввиду очевидности его интерпретации в каждом случае применения. Операцию умножения векторов $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ и $x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}$ определим по правилу «умножения многочленов»:

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}) = ax\mathbf{e}\circ\mathbf{e} + ay\mathbf{e}\circ\mathbf{i} + az\mathbf{e}\circ\mathbf{j} + aw\mathbf{e}\circ\mathbf{k} + bx\mathbf{i}\circ\mathbf{e} + by\mathbf{i}\circ\mathbf{i} + bz\mathbf{i}\circ\mathbf{j} + bw\mathbf{i}\circ\mathbf{k} + cx\mathbf{j}\circ\mathbf{e} + cy\mathbf{j}\circ\mathbf{i} + cz\mathbf{j}\circ\mathbf{j} + cw\mathbf{j}\circ\mathbf{k} + dx\mathbf{k}\circ\mathbf{e} + dy\mathbf{k}\circ\mathbf{i} + dz\mathbf{k}\circ\mathbf{j} + dw\mathbf{k}\circ\mathbf{k},$$

где координаты вектора умножаются как элементы кольца $\mathbb{Z}_m$, а операция ∘ имеет более высокий приоритет по сравнению со сложением, и произведения всевозможных пар базисных векторов заменяются базисным вектором или однокомпонентным вектором в соответствии с правилом умножения, задаваемым табл. 1, в которой параметр $\varepsilon \in \mathbb{Z}_m$ называется коэффициентом растяжения, разные значения которого задают разные варианты операции умножения четырехмерных векторов. Таким образом, определенная операция умножения векторов (a, b, c, d) и (x, y, z, w) выполняется по правилу

$$(a, b, c, d) \circ (x, y, z, w) = (ax + \varepsilon bw + \varepsilon cz + \varepsilon dy)\mathbf{e} + (ay + bx + cw + dz)\mathbf{i} + (az + \varepsilon by + cx + dw)\mathbf{j} + (aw + \varepsilon bz + \varepsilon cy + dx)\mathbf{k}.$$

Легко проверить, что определенная операция умножения обладает свойствами ассоциативности и коммутативности, а нейтральным элементом по умножению является вектор $E = (1, 0, 0, 0)$.

Множество всех векторов $\{A\}$ такое, что каждому вектору A может быть сопоставлен обратный вектор A^{-1}, для которого выполняется соотношение $AA^{-1} = E$, образует конечную группу. Значение ее порядка Ω определяется выбором значений m и ε. Рассмотрим решение уравнений вида $AX = E$, которое можно представить следующим образом:

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}) = (ax + \varepsilon bw + \varepsilon cz + \varepsilon dy)\mathbf{e} + (ay + bx + cw + dz)\mathbf{i} + (az + \varepsilon by + cx + dw)\mathbf{j} + (aw + \varepsilon bz + \varepsilon cy + dx)\mathbf{k} = 1\mathbf{e} + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}.$$

Из последней записи вытекает, что для определения обратных значений следует решать следующую систему из четырех линейных сравнений с четырьмя неизвестными:

$$\begin{cases} ax + \varepsilon dy + \varepsilon cz + \varepsilon bw \equiv 1 \bmod m \\ bx + ay + dz + cw \equiv 0 \bmod m \\ cx + \varepsilon by + az + dw \equiv 0 \bmod m \\ dx + \varepsilon cy + \varepsilon bz + aw \equiv 0 \bmod m \end{cases}. \qquad (1)$$

■ ***Таблица 1.*** *Правила умножения четырехмерных базисных векторов*

Базисные векторы	Базисные векторы			
	e	**i**	**j**	**k**
e	**e**	**i**	**j**	**k**
i	**i**	ε**j**	ε**k**	ε**e**
j	**j**	ε**k**	ε**e**	**i**
k	**k**	ε**e**	**i**	**j**

Формирование конечных нециклических групп с требуемыми значениями порядка обеспечим выбором значения m, равного квадрату простого числа p, и выбором соответствующего значения коэффициента ε.

Утверждение 1. Пусть $m = p^2$, где p — простое число и $p \geq 3$. При значении $\varepsilon < p^2$ таком, что $p|\varepsilon$, формируется группа Г четырехмерных векторов, порядок которой $\Omega = p^7(p-1)$.

Доказательство: Рассмотрим множество векторов (a, b, c, d) таких, что $a \neq 0$ и a не делится на p. При условиях утверждения 1 главный определитель Δ системы сравнений (1), записанной для рассматриваемых векторов, является взаимно простым с модулем p^2. Покажем, что определитель представи́м в виде $\Delta = a^4 + pQ$ при некотором целом числе Q. Для этого запишем определитель в виде суммы произведений всех элементов его первой строки на их алгебраические дополнения:

$$\Delta = aA_a + \varepsilon dA_{\varepsilon d} + \varepsilon cA_{\varepsilon c} + \varepsilon bA_{\varepsilon b} = aA_a + \varepsilon Q',$$

где Q' — целое число и алгебраическое дополнение элемента a

$$A_a = a(a^2 - \varepsilon bd) - \varepsilon b(a^2 - \varepsilon c^2) + \\ + \varepsilon c(a^2 - \varepsilon bd) = a^3 + \varepsilon Q'',$$

здесь Q'' — целое число. Следовательно: $\Delta = a^4 + \varepsilon Q^*$, и в силу делимости ε на p получаем $\Delta = a^4 + pQ$, где Q^* и Q — целые числа. Поскольку для рассматриваемых векторов $a \neq 0$ и простое p не делит a, то p не делит a^4, следовательно, p не делит Δ, т. е. наибольший общий делитель Δ и p^2 равен 1, поэтому существует значение Δ^{-1} такое, что $\Delta^{-1}\Delta \equiv 1 \bmod p^2$. Таким образом, для каждого из рассматриваемых векторов система (1) имеет решение, т. е. эти векторы являются обратимыми. При этом операция умножения двух векторов дает третий вектор, в котором первая координата также не делится на p, т. е. операция умножения является замкнутой на рассматриваемом множестве векторов (a, b, c, d). Следовательно, это множество является группой, порядок которой можно определить из того факта, что число возможных значений первой координаты равно функции Эйлера от модуля $\varphi(p^2) = p(p-1)$, а число возможных значений второй, третьей и четвертой координат равно p^2. Получаем следующую формулу для значения порядка построенной мультипликативной группы:

$$\Omega = p(p-1)\cdot p^2 \cdot p^2 \cdot p^2 = p^7(p-1).$$

Легко видеть, что в рассматриваемом множестве четырехмерных векторов нет другой группы Г′, в которую включена построенная группа Г в качестве подгруппы. Действительно, порядок группы делится на порядок своей подгруппы. Поэтому если бы существовала указанная группа Г″, то ее порядок Ω″ должен был бы быть равным или превышать значение $2\Omega = 2p^7(p-1)$. Но этого быть не может при $p \geq 3$, так как число ненулевых векторов равно $p^8 - 1$. Утверждение доказано.

Согласно теореме Силова [7], в группах, соответствующих условиям утверждения 1, содержатся подгруппы порядка, равного всем степеням числа p от 2 до 7, причем известна теорема, что любая подгруппа простого порядка является циклической, т. е. в построенной группе существуют циклические группы порядка p. Однако нас интересуют нециклические группы, содержащие циклические подгруппы, порядок которых делится на квадрат простого числа. Поэтому важным является выяснение вопроса существования циклических подгрупп порядка $p^2, p^3, \ldots, p^7$.

Утверждение 2. Максимальным значением порядка элементов группы Г является значение $\omega_{\max} = p^2(p-1)$.

Доказательство: Покажем, что в группе Г содержатся векторы порядка $p^2(p-1)$. Рассмотрим вектор $G_1 = (a, 0, c, 0) = a\mathbf{e} + c\mathbf{j}$, где a — первообразный корень по модулю p^2 и $1 \leq c \leq p-1$. Возведем G_1 в степень s, используя формулу бинома Ньютона. Учитывая, что $\varepsilon^r = 0$ при $r \geq 2$, $\mathbf{j}^r = 0$ (ноль — значение векторного пространства) при $r \geq 4$, $\mathbf{j}^2 = \varepsilon\mathbf{e}$ и $\mathbf{j}^3 = \varepsilon\mathbf{j}$, получим

$$(a\mathbf{e} + c\mathbf{j})^s = a^s\mathbf{e} + sa^{s-1}c\mathbf{j} + \\ + \frac{s(s-1)}{2}a^{s-2}c^2\varepsilon\mathbf{e} + \frac{s(s-1)(s-2)}{2\cdot 3}a^{s-3}c^3\varepsilon\mathbf{j} = \\ = \left(a^s + \frac{s(s-1)}{2}a^{s-2}c^2\varepsilon\right)\mathbf{e} + \\ + \left(sa^{s-1}c + \frac{s(s-1)(s-2)}{2\cdot 3}a^{s-3}c^3\varepsilon\right)\mathbf{j}.$$

Учитывая, что $p|\varepsilon$, скобка при $\mathbf{e}$ может быть равна 1 только в случае, когда в ней первое слагаемое (a^s) равно 1, а второе равно 0. Минимальное значение s, при котором это возможно, равно $p(p-1)$, поскольку a — первообразный корень по модулю p^2. При этом скобка при $\mathbf{j}$ не равна 0, так как c не делится на p и второе слагаемое в этой скобке делится на p^2. Минимальное значение s, при котором вторая скобка равна нулю, равно p^2. Таким образом: $(a\mathbf{e} + c\mathbf{j})^s = (1, 0, 0, 0) = \mathbf{e}$ при $s = p^2(p-1)$ и $(a\mathbf{e} + c\mathbf{j})^s \neq \mathbf{e}$ при $s < p^2(p-1)$, т. е. порядок рассматриваемого вектора равен $p^2(p-1)$. Легко видеть, что при произвольных значениях a и c имеем $G_1^{p^2(p-1)} = \mathbf{e}$.

Возведем вектор $G_1 + b\mathbf{j}$, где b — произвольное значение, в степень s, используя формулу бинома Ньютона. Учитывая, что $\mathbf{i}^r = 0$ при $r \geq 3$, $\mathbf{i}^2 = \varepsilon\mathbf{j}$:

$$(G_1 + b\mathbf{i})^s = G_1^s + sG_1^{s-1}b\mathbf{i} + \frac{s(s-1)}{2}G_1^{s-2}b^2\varepsilon\mathbf{j}.$$

При $s = p^2(p-1)$ правая часть последнего выражения равна (1, 0, 0, 0), т. е. все векторы вида $V = G_1 + b\mathbf{j}$ имеют порядок не больше значения $p^2(p-1)$. Возведем вектор $V + d\mathbf{k}$ при произвольном d в степень $p^2(p-1)$, учитывая, что $\mathbf{k}^r = 0$ при $r \geq 8$ и то, что все слагаемые, содержащие множитель p^2, также равны нулю:

$$(V + d\mathbf{k})^{p^2(p-1)} = V^{p^2(p-1)} + p^2(p-1)\times$$

$$\times V^{p^2(p-1)-1}d\mathbf{k} + 0 + 0 + \ldots + 0 = V^{p^2(p-1)} = \mathbf{e}.$$

Таким образом, для всех четырехмерных векторов Z группы Г выполняется условие $Z^{p^2(p-1)} = \mathbf{e}$, т. е. $\omega_{\max} = p^2(p-1)$. Утверждение 2 доказано.

Из утверждений 1 и 2 вытекает, что коммутативная группа Г не может быть порождена одним элементом, т. е. она не является циклической. Известно ([8], с. 66–73), что конечные коммутативные группы являются прямым произведением примарных циклических подгрупп. Если взять из каждой такой подгруппы генератор, то их совокупность будет образовывать примарный базис — набор элементов, порядок которых равен степени простого числа, причем любой элемент группы может быть представлен единственным способом как произведение степеней элементов указанного набора. Элементы базиса, порядки которых являются взаимно простыми, порождают циклические подгруппы. Два или более таких элементов базиса можно заменить генератором порождаемой ими «непримарной» циклической подгруппы, т. е. количество элементов в базисе может быть различным, если не требовать того, чтобы базис был примарным (существует большое число различных примарных базисов, но число элементов в них является одинаковым).

Покажем, что рассматриваемая группа Г порождается базисом, включающим один элемент порядка $p(p-1)$ и три элемента порядка p^2. Элементом порядка $p(p-1)$ является вектор $B_1 = (a, 0, 0, 0)$, где a — первообразный корень по модулю p^2. В качестве базисных элементов порядка p^2 возьмем следующие три вектора: $B_2 = (a', b, 0, 0)$, $B_3 = (a', 0, c, 0)$ и $B_4 = (a', 0, 0, d)$, где a' — число порядка p по модулю p^2 и числа b, c и d не делятся на p. Записывая степени элементов B_1, B_2, B_3 и B_4 по формуле бинома Ньютона, легко показать, что их порядки равны заявленным значениям и порождаемые этими элементами циклические подгруппы пересекаются только в единичном элементе. Следовательно, их прямое произведение включает $p(p-1)p^2p^2p^2 = \Omega$ различных элементов, т. е. на самом деле векторы B_1, B_2, B_3 и B_4 составляют базис нециклической группы Г, строение которой можно охарактеризовать в терминах многомерной цикличности. Как показано выше, максимальный порядок циклических подгрупп, содержащихся в группе Г, составляет $\Omega_{\max}^{\text{цикл}} = p^2(p-1)$, т. е. порядок циклических групп делится на квадрат простого числа p, которое можно использовать в качестве степени корня, что делает эти группы перспективными для решения нашей задачи синтеза алгоритмов ЭЦП, основанных на вычислительной сложности нахождения корней p-й степени и обеспечивающих повышение про-

■ ***Таблица 2.*** *Строение частных вариантов конечных групп* Г *четырехмерных векторов над кольцом* $\mathbb{Z}_{p^2}$ (N_ω — *число элементов порядка* ω)

$p = 23^2$; $\varepsilon = 23$		$p = 7^2$; $\varepsilon = 14$		$p = 5^2$; $\varepsilon = 15$		$p = 11^2$; $\varepsilon = 22$	
ω	N_ω	ω	N_ω	ω	N_ω	ω	N_ω
2	1	2	1	2	1	2	1
11	10	3	2	4	2	5	4
22	10	6	2	5	624	10	4
23	279840	7	2400	10	624	11	14640
46	279840	14	2400	20	1248	22	14640
253	2798400	21	4800	25	77500	55	58560
506	2798400	42	4800	50	77500	110	58560
529	3404545606	49	821142	100	155000	121	19472530
1058	3404545606	98	821142	–	–	242	19472530
5819	34045456060	147	1642284	–	–	605	77890120
11638	34045456060	294	1642284	–	–	1210	77890120
$1+\sum_{\omega} N_\omega$	74906159834	–	4941258	–	312500	–	19487171
$p^7(p-1)$	74906159834	–	4941258	–	312500	–	194871710

изводительности по сравнению с алгоритмами, предложенными в работах [3, 4].

Для определения детального строения частных случаев групп Г был выполнен вычислительный эксперимент с помощью специально разработанной программы для ЭВМ, в котором для заданного значения p определялся порядок каждого обратимого четырехмерного вектора и подсчитывалось число векторов, обладающих каждым возможным значением порядка. Эксперимент (табл. 2) подтвердил, что группы, соответствующие условиям утверждения 1, являются нециклическими и их строение согласуется с ранее полученными результатами по исследованию строения конечных групп многомерных векторов, заданных над простым полем [6]. В частности из табл. 2 видно, что группа Г содержит подгруппу порядка p^4, содержащую $p^4 - 1$ элементов порядка p и обладающую однородной (ее базис включает элементы равного порядка) четырехмерной цикличностью своего строения. Последние две строки таблицы иллюстрируют проверку полученных результатов.

Оценка сложности задачи извлечения корней в группах векторов

Оценка сложности задачи извлечения корней простой степени p в группах Г требует выбора наиболее эффективного известного алгоритма решения этой задачи. Из приводимых в литературе алгоритмов решения этой задачи в мультипликативной группе поля GF(p) при $p = Nk^2 + 1$ наименьшую вычислительную сложность при $|k| < 160$ бит и $|p| > 1024$ бит имеет алгоритм непосредственного вычисления корней [3], а при $|k| > 160$ бит и $|p| < 1024$ бит — алгоритм, включающий предварительное вычисление дискретного логарифма элемента, из которого вычисляется корень степени k [4]. Аналогичные алгоритмы вычисления корней могут быть построены и для рассматриваемых групп четырехмерных векторов с учетом строения этих групп. В общем случае векторов произвольной размерности, заданных над простыми полями, их строение детально рассмотрено в работе [6], где показано, что конечные группы векторов характеризуются строением, описываемым в терминах многомерной цикличности.

Интерпретация полученных экспериментальных и теоретических результатов по построенным в предыдущем разделе группам четырехмерных векторов в терминах многомерной цикличности и использование формул для определения количества элементов группы, имеющих заданное значение порядка, позволяет определить количество циклических подгрупп каждого возможного значения порядка. Кроме того, из полученных экспериментальных результатов следует, что рассматриваемые группы четырехмерных векторов имеют четырехмерную цикличность и элементы группы могут быть порождены некоторыми четверками элементов, например G_1, G_2, G_3 и G_4, как произведения некоторых степеней этой системы порождающих, состоящей из указанных четырех элементов. Таким образом, любой четырехмерный вектор A, принадлежащий группе Г, может быть представлен в виде $A = G_1^i \circ G_2^j \circ G_3^h \circ G_4^u$, где i, j, h и u — целочисленные степени, причем $i, j, h, u < \Omega_{\max}^{\text{цикл}}$.

Предположим, что для элемента $Y = G_1^{i_y} \circ \circ G_2^{j_y} \circ G_3^{h_y} \circ G_4^{u_y}$ уравнение $X = \sqrt[p]{Y}$ имеет решение. Пусть решением является некоторый вектор $X = G_1^{i_x} \circ G_2^{j_x} \circ G_3^{h_x} \circ G_4^{u_x}$. Тогда имеем

$$X^p = \left(G_1^{i_x} \circ G_2^{j_x} \circ G_3^{h_x} \circ G_4^{u_x} \right)^p =$$

$$= G_1^{pi_x} \circ G_2^{pj_x} \circ G_3^{ph_x} \circ G_4^{pu_x} =$$

$$= G_1^{i_y} \circ G_2^{j_y} \circ G_3^{h_y} \circ G_4^{u_y}.$$

Из последнего соотношения легко видеть, что вычисление корня можно свести к вычислению дискретного логарифма по четырехмерному основанию (G_1, G_2, G_3, G_4). Решение последней задачи даст значение четырехмерного логарифма от Y, равное (i_y, j_y, h_y, u_y) = (pi_x, pj_x, ph_x, pu_x), из которого легко найти (i_x, j_x, h_x, u_x) и $X = G_1^{i_x} \circ G_2^{j_x} \circ G_3^{h_x} \circ G_4^{u_x}$. Рассмотрим следующий алгоритм вычисления четырехмерного логарифма и оценим его трудоемкость.

1. Вычислить значения $V_1 = Y \circ G_1^{-i} \circ G_2^{-j}$ для всех i, $j \le \Omega_{\max}^{\text{цикл}}$ и запомнить их в некотором массиве М1 (трудоемкость этого шага W_1 примерно равна $W_1 = \omega^2$ операций возведения в степень, где $\omega = \Omega_{\max}^{\text{цикл}}$).

2. Упорядочить массив М1 по значениям V_1 (трудоемкость этого шага равна $W_2 \approx \omega^2 \log_2 \omega^2$ операций сравнения).

3. Последовательно для $h = 0, 1, 2, \ldots, \omega$ и $u = 0, 1, 2, \ldots, \omega$ вычислять $V_2 = G_3^h \circ G_4^u$ и проверять, имеется ли такое значение в массиве М1, пока для некоторой пары значений $h = h_0$ и $u = u_0$ не будет получено значение $V_2 = G_3^{h_0} \circ G_4^{u_0}$, присутствующее в М1 как значение V_1 и соответствующее некоторой паре значений $i = i_0$ и $j = j_0$ (трудоемкость этого шага W_3 не превышает $\omega^2 \log_2 \omega^2$ операций сравнения и ω^2 операций возведения в степень).

После завершения работы алгоритма имеем $Y = G_1^{i_0} \circ G_2^{j_0} \circ G_3^{h_0} \circ G_4^{u_0}$ и $X = G_1^{\frac{i_0}{p}} \circ G_2^{\frac{j_0}{p}} \circ G_3^{\frac{h_0}{p}} \circ G_4^{\frac{u_0}{p}}$. В целом трудоемкость этого алгоритма можно оценить как $O(\omega^2) = O(p^4(p-1)^2)$ операций возведения в степень (операции сравнения имеют меньшую сложность), где $O(*)$ — обозначение порядка

величины *. Можно свести задачу нахождения четырехмерного логарифма в исходной группе к задаче нахождения четырехмерного логарифма в подгруппе порядка p^4, имеющей четырехмерное циклическое строение. В последнем случае логарифм находится с помощью алгоритма, аналогичного рассмотренному выше, но имеющему значительно меньшую трудоемкость — $O(p^2)$ операций возведения в степень.

Рассмотрим алгоритм непосредственного вычисления корня p-й степени. Легко видеть, что $X^{\omega} = Y^{\omega/p} = E$, где $\omega = \Omega_{\max}^{\text{цикл}}$ и E — единичный вектор, поэтому имеем $Y^{\frac{\omega}{p^2}} = E^{\frac{1}{p}}$. В рассматриваемой группе содержится подгруппа Γ_4 порядка p^4, все элементы которой, кроме единичного, имеют порядок p и являются корнями p-й степени из единичного элемента. Четыре случайно выбранных элемента G_{E1}, G_{E2}, G_{E3} и G_{E4} порядка p (их можно найти по способу, описанному в работе [9], с. 20–21, в виде $G_{E1} = B_1^{\omega/p}$, $G_{E2} = B_2^{\omega/p}$, $G_{E3} = B_3^{\omega/p}$ и $G_{E4} = B_4^{\omega/p}$, где B_1, B_2, B_3 и B_4 — векторы порядка ω) с вероятностью, близкой к 1, будут принадлежать различным подгруппам и составят четырехмерный генератор подгруппы Γ_4, т. е. систему образующих, состоящую из четырех различных векторов порядка p. При некоторых степенях i, j, h и u выполняется $Y^{\frac{\omega}{p^2}} = G_{E1}^{i} \circ G_{E2}^{j} \circ G_{E3}^{h} \circ G_{E4}^{u}$. Это соотношение лежит в основе следующего алгоритма.

1. Вычислить значения $V_1 = Y^{\frac{\omega}{p^2}} \circ G_{E1}^{-i} \circ G_{E2}^{-j}$ для всех $i \le p$ и $j \le p$ и запомнить их в некотором массиве M1 (трудоемкость этого шага W_1 равна p^2 операций возведения в степень).

2. Упорядочить массив M1 по значениям V_1 (трудоемкость этого шага равна $W_2 \approx p^2 \log_2 p^2$ операций сравнения).

3. Последовательно для $h = 0, 1, 2, \ldots, p$ и $u = 0, 1, 2, \ldots, p$ вычислять $V_2 = G_{E3}^{h} \circ G_{E4}^{u}$ и проверять, имеется ли такое значение в массиве M1, пока для некоторой пары значений $h = h_0$ и $u = u_0$ не будет получено значение $V_2 = G_{E3}^{h_0} \circ G_{E4}^{u_0}$, присутствующее в M1 как значение $V_1 = Y^{\frac{\omega}{p^2}} \circ G_{E1}^{-i_0} \circ G_{E2}^{-j_0}$, соответствующее некоторым показателям степеней $i = i_0$ и $j = j_0$ (трудоемкость этого шага равна $W_3 \le O(p^2 \log_2 p^2)$ операций сравнения и $O(p^2)$ операций возведения в степень).

В целом трудоемкость этого алгоритма равна $O(p^2)$ операций возведения в степень. При значениях $|p| \ge 40$ бит найти корни простой степени p в рассматриваемых нециклических группах вычислительно невозможно, поскольку это требует совершения более 2^{80} операций возведения в степень. После выполнения алгоритма имеем

$$Y^{\frac{\omega}{p^2}} = G_{E1}^{i_0} \circ G_{E2}^{j_0} \circ G_{E3}^{h_0} \circ G_{E4}^{u_0} =$$

$$= B_1^{\frac{\omega}{p^2} i_0 p} \circ B_2^{\frac{\omega}{p^2} j_0 p} \circ B_3^{\frac{\omega}{p^2} h_0 p} \circ B_4^{\frac{\omega}{p^2} u_0 p} \Rightarrow Y^{\frac{\omega}{p^2}+p} =$$

$$= B_1^{\frac{\omega}{p^2} i_0 p} \circ B_2^{\frac{\omega}{p^2} j_0 p} \circ B_3^{\frac{\omega}{p^2} h_0 p} \circ B_4^{\frac{\omega}{p^2} u_0 p} \circ Y^{p}. \quad (2)$$

Легко видеть, что $\text{НОД}(\omega, \psi) = 1$, где $\psi = p + \frac{\omega}{p^2}$ — целое число, поэтому существует и легко вычисляется значение $t = \psi^{-1} \bmod \omega$. Из (2) получаем формулу для определения искомого корня

$$Y = \left(B_1^{\frac{\omega}{p^2} i_0 t} \circ B_2^{\frac{\omega}{p^2} j_0 t} \circ B_3^{\frac{\omega}{p^2} h_0 t} \circ B_4^{\frac{\omega}{p^2} u_0 t} \circ Y^{t} \right)^{p} \Rightarrow$$

$$\Rightarrow \sqrt[p]{Y} = B_1^{\frac{\omega}{p^2} i_0 t} \circ B_2^{\frac{\omega}{p^2} j_0 t} \circ B_3^{\frac{\omega}{p^2} h_0 t} \circ B_4^{\frac{\omega}{p^2} u_0 t} \circ Y^{t}. \quad (3)$$

Завершающие вычисления по формулам (2) и (3) не влияют на полученную оценку трудоемкости алгоритма непосредственного вычисления корней. Формула (3) дает одно значение корня, все остальные корни из Y могут быть найдены путем умножения полученного корня $\sqrt[p]{Y}$ на все корни из единичного вектора E. Это легко доказывается. Очевидно, что все корни $\sqrt[p]{Y}$ эквивалентны для рассмотренной ниже схемы ЭЦП, но это не критично для ее стойкости, поскольку их доля как элементов группы Γ составляет при используемых длинах простого числа p пренебрежимо малую величину, равную

$$\frac{p^4}{\Omega} = \frac{p^4}{p^7(p-1)} = \frac{1}{p^3(p-1)}.$$

Приведенные выше алгоритмы вычисления корня степени p легко записать и для общего случая μ-мерного циклического строения группы векторов и получить следующую формулу для сложности вычисления корня степени p:

$$W_{\mu} = O\left(\sqrt{p^{\mu}}\right). \quad (4)$$

Алгоритм электронной цифровой подписи

Рассмотренная выше нециклическая группа четырехмерных векторов может быть использована для построения алгоритмов ЭЦП, основанных на сложности задачи нахождения корней большой простой степени k в конечных группах известного порядка. Для этой цели в качестве степени выбирается простое значение p такое, что $|p| \ge 40$ бит. Рассмотрим построение алгоритма ЭЦП. В качестве секретного ключа использу-

ется пара векторов X_1 и X_2 группы Г таких, что их порядки равны $\omega(X_1) = \omega_{max}$ и $\omega(X_2) = \omega_{max} = p^2(p-1)$. Генерация векторов X максимального порядка ω_{max} осуществляется следующим путем. Выбирается случайный вектор W такой, что $W^{p^2(p-1)} = E$, и для всех простых делителей δ числа ω_{max} вычисляется вектор $V = W^{p^2(p-1)/\delta}$. Если для всех δ выполняется $V \neq E$, то W берется в качестве X.

Открытый ключ представляет собой пару четырехмерных векторов, генерируемых по формулам $Y_1 = X_1{}^p$ и $Y_2 = X_2{}^p$. Необходимость использовать в качестве открытого ключа два вектора Y_1 и Y_2 связана с тем, что в силу правила их вычисления их порядок равен 80-битовому (при $|p| = 40$ бит) значению $\omega_Y = p(p-1)$. Последнее означает, что возведение одного открытого ключа, используемого в качестве одного из параметров процедуры проверки подлинности ЭЦП, в степень, равную 160-битовому значению хэш-функции E, дает тот же результат, что и возведение этого ключа в степень, равную 80-битовому значению $E \bmod \omega_Y$. Чтобы устранить эффект урезания «эффективной» длины хэш-функции, в приводимой ниже схеме ЭЦП используются два вектора в качестве открытого ключа, а значение E представляется в виде конкатенации двух 80-битовых значений e_1 и e_2, используемых при верификации ЭЦП как степени, в которые возводятся открытые ключи Y_1 и Y_2 соответственно.

Процедура генерации ЭЦП состоит в следующем.

1. Выбирается случайный элемент T группы Г такой, что $\omega(T) \geq p^2$.

2. Вычисляется значение $R = T^p$.

3. Вычисляется значение хэш-функции F_H от подписываемого документа M, к которому предварительно присоединяются координаты r_1, r_2, r_3 и r_4 элемента R: $E = F_H(M\|r_1\|r_2\|r_3\|r_4)$, где $\|$ — операция конкатенации. Значение E является первым элементом ЭЦП. Пусть, например, размер E равен 160 бит. Значение E представляется в виде конкатенации двух 80-битовых чисел: $E = e_1\|e_2$.

4. Вычисляется второй элемент ЭЦП: $S = T \circ X_1^{e_1} \circ X_2^{e_2}$.

Сформированная ЭЦП (E, S) включает два элемента, первый из которых является числом, а второй — элементом группы Г, т. е. четырехмерным вектором. Проверка подлинности ЭЦП осуществляется следующим образом.

1. Вычисляется значение $R' = Y_1^{\omega - e_1} \circ Y_2^{\omega - e_2} \circ S^p$.

2. Вычисляется значение хэш-функции $E' = F_H(M\|r'_1\|r'_2\|r'_3\|r'_4)$, где r'_1, r'_2, r'_3 и r'_4 — координаты вектора $R' \in \Gamma$.

3. Сравниваются значения E и E'. Если $E = E'$, то ЭЦП признается подлинной.

■ ***Таблица 3.*** *Сравнение производительности алгоритмов ЭЦП*

Алгоритм ЭЦП	Размер ЭЦП, бит	Размер ОК, бит	Производительность, отн. ед.
ГОСТ Р 34.10-94	320*	1024	1
ГОСТ Р 34.10-2001	320*	320*	3,5
ECDSA	320	320	3,5
Предложенный ($\|p\| \approx 40$ бит)	480	640	10

* В спецификации стандартов рекомендуются размеры значений ЭЦП и открытого ключа (ОК), превышающие 320 бит, что дает стойкость более 2^{80}.

Стойкость данного алгоритма ЭЦП определяется сложностью задачи извлечения корней, рассмотренной выше.

Сопоставление с известными алгоритмами

Сравнительная оценка производительности различных алгоритмов ЭЦП в случае уровня безопасности, равного 2^{80} операциям возведения в степень, представлена в табл. 3.

Алгоритм ГОСТ Р 34.10-94 основан на сложности дискретного логарифмирования в конечном простом поле, алгоритмы ГОСТ Р 34.10-2001 и ECDSA — на сложности дискретного логарифмирования в конечной группе точек эллиптической кривой (ЭК), а предложенный — на основе сложности задачи извлечения корней в нециклических группах, рассмотренных в данной статье. Более высокая производительность предложенного алгоритма обеспечивается тем, что в нем вычисления выполняются над элементами существенно меньшего размера по сравнению с первым алгоритмом, а групповая операция свободна от операции инверсии, которая присутствует как составная часть в операции сложения точек ЭК.

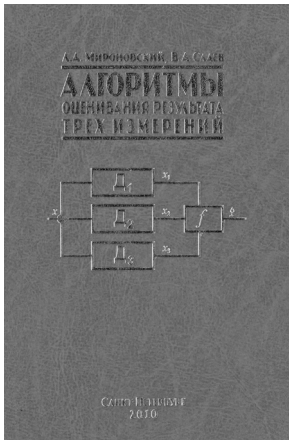
Заключение

Для синтеза алгоритмов ЭЦП, основанных на вычислительной сложности задачи нахождения корней большой простой степени в конечных группах известного порядка, предложены нециклические конечные группы четырехмерных векторов, координатами которых являются элементы кольца вычетов по модулю, равному квадрату простого числа p. Получена формула, выражающая порядок группы через значение p. Представлена схема ЭЦП, обладающая существенно более высокой производительностью по сравнению с известными алгоритмами ЭЦП.

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

Литература

1. **Молдовян Н. А.** Алгоритмы аутентификации информации в АСУ на основе структур в конечных векторных пространствах // Автоматика и телемеханика. 2008. № 12. С. 163–177.
2. **Доронин С. Е., Молдовян Н. А., Синев В. Е.** Конечные расширенные поля для алгоритмов электронной цифровой подписи // Информационно-управляющие системы. 2009. № 1. С. 33–40.
3. **Молдовян Н. А.** Извлечение корней по простому модулю как криптографический примитив // Вестник СПбГУ. Сер. 10. 2008. Вып. 1. С. 100–105.
4. **Молдовян А. А., Молдовян Н. А.** Новые алгоритмы и протоколы для аутентификации информации в АСУ // Автоматика и телемеханика. 2008. № 7. С. 157–169.
5. **Гурьянов Д. Ю., Дернова Е. С., Избаш В. И., Молдовян Д. Н.** Алгоритмы электронной цифровой подписи на основе сложности извлечения корней в конечных группах известного порядка // Информационно-управляющие системы. 2008. № 5. С. 33–40.
6. **Молдовян Н. А.** Аутентификация информации в АСУ на основе конечных групп с многомерной цикличностью // Автоматика и телемеханика. 2009. № 8. С. 177–190.
7. **Каргаполов М. И., Мерзляков Ю. И.** Основы теории групп. — М.: Физматлит, 1996. — 287 с.
8. **Кострикин А. И.** Введение в алгебру: Ч. 3. Основные структуры алгебры. — М.: Физико-математическая литература, 2001. — 271 с.
9. **Молдовян Н. А.** Практикум по криптосистемам с открытым ключом. — СПб.: БХВ-Петербург, 2007. — 298 с.



Мироновский Л. А., Слаев В. А. Алгоритмы оценивания результата трех измерений. — СПб.: «Профессионал», 2010. — 192 с.: ил. ISBN 978-5-91259-041-2, УДК 389.

Монография состоит из пяти глав и трех приложений. В ней собраны, классифицированы и проанализированы алгоритмы оценивания, направленные на решение «задачи о трех измерениях».

В Главе I приведена классификация погрешностей измерений, а также методов оценивания, оптимизирующих выбранные критерии. Эти методы по виду критериев подразделяются на вероятностные, детерминированные, эвристические и диагностические. Описаны классические средние оценки и их свойства.

Глава II посвящена вероятностному и детерминированному подходам к оцениванию. В ней рассмотрены оценки максимального правдоподобия, марковские, байесовские, квадратические, модульные и степенные оценки, а также оценки, оптимизирующие составные и комбинированные критерии.

Глава III описывает принципы эвристического оценивания, основанные на математическом определении средних величин по Коши и Колмогорову. На этом пути строятся классические средние, линейные, квазилинейные, а также разностные квазилинейные и нелинейные оценки.

В Главе IV рассматриваются диагностические методы получения оценок, основанные на применении алгебраических инвариантов. Наличие алгебраических инвариантов позволяет осуществить отбраковку искаженных измерений методами технической диагностики по минимальному или максимальному рассогласованию. Алгоритмы оценивания скалярной величины по трем измерениям сведены в таблицу, в которой отражено более семидесяти различных оценок.

Глава V касается применения средних оценок для фильтрации сигналов. Охарактеризован принцип использования «гладкости» сигналов для борьбы с погрешностями, применение которого приводит к фильтрам с конечной памятью. Описаны медианные и диагностические фильтры, приведен пример фильтрации навигационной информации.

В Приложения вынесены современная терминология по характеристикам точности, соотношение между неопределенностями и характеристиками погрешности, а также статистические свойства получаемых оценок.

Для метрологов, приборостроителей и разработчиков алгоритмов, реализуемых в программно управляемых средствах измерений, а также для экспертов, осуществляющих их аттестацию. Может быть полезна студентам и аспирантам технических вузов.

Книгу можно приобрести за наличный и безналичный расчет во ВНИИМ им. Д. И. Менделеева: 190005, Санкт-Петербург, Московский пр., 19; контактный телефон +7 (812) 323-93-79;
e-mail: abl@bi10.vniim.ru, Любомиров Андрей Борисович. Цена экземпляра 413 руб.