имеющие малый размер. Для задания групп векторов могут быть использованы распределения коэффициентов растяжения, определяемые таблицами 1 и 2, причем таблица 2 минимизирует число операций в поле $GF(p^s)$.

Представлен общий подход к построению схем ЭЦП на основе групп с многомерной цикличностью и предложен конкретный алгоритм. Вопрос оценки безопасного размера порядка групп векторов, используемых для построения алгоритмов ЭЦП, представляет собой самостоятельную задачу, связанную с нахождением эффективных способов вычисления многомерных дискретных логарифмов.

СПИСОК ЛИТЕРАТУРЫ:

1. *Венбо Мао*. Современная криптография. Теория и практика. М.; СПб.; Киев: Издательский дом «Вильямс», 2005. — 763 с.
2. *Молдовян Н. А.* Практикум по криптосистемам с открытым ключом. СПб.: БХВ-Петербург, 2007. — 298 с.
3. *Menezes A. J., Vanstone S. A.* Elliptic Curve Cryptosystems and Their Implementation // Journal of cryptology. 1993. Vol. 6. № 4. P. 209–224.
4. *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.
5. *Болотов А. А., Гашков С. Б., Фролов А. Б.* Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006. — 274 с.
6. *Молдовяну П. А., Дернова Е. С., Молдовян Д. Н.* Синтез конечных расширенных полей для криптографических применений // Вопросы защиты информации. 2008. № 3 (82). С. 2–7.
7. *Молдовян Н. А.* Многомерная цикличность групп векторов и их использование в алгоритмах аутентификации информации // Вестник СПбГУ. Серия 10. 2009 (в печати).
8. *Молдовян Д. Н., Молдовяну П. А.* Задание умножения в полях векторов большой размерности // Вопросы защиты информации. 2008. № 3 (82). С. 12–17.
9. *Menezes A. J., Van Oorschot P. C., Vanstone S. A.* Handbook of Applied Cryptography. CRC Press, Boca Raton, FL, 1997. — 780 p.

Н. А. Молдовян, П. А. Молдовяну

СЛОЖНОСТЬ ВЫЧИСЛЕНИЯ КОРНЕЙ В КОНЕЧНЫХ ГРУППАХ ИЗВЕСТНОГО ПОРЯДКА КАК КРИПТОГРАФИЧЕСКИЙ ПРИМИТИВ[1]

Введение

В специальных частных случаях [1] задача извлечения корней большой простой степени в конечных полях простого порядка является вычислительно сложной и может быть положена в основу алгоритмов электронной цифровой подписи. Предложенные в работе [1, 2] схемы ЭЦП основаны на вычислениях в поле, порядок которого имеет размер 1024 бит и более (здесь и далее под размером некоторой величины понимается ее разрядность в двоичном представлении), в связи с тем, что задача извлечения корней в указанном поле может быть решена путем предварительного вычисления дискретного логарифма. Последнее означает, что сложность дискретного логарифмирования ограничивает сверху безопасность алгоритмов ЭЦП, основанных на трудности извлечения корней в полях простого порядка [2]. Для повышения вычислительной эффективности схем ЭЦП, основанных на сложности вычисления корней, представляют интерес конечные группы,

[1] Работа выполнена при поддержке РФФИ, грант № 08-07-00096-а.

в которых указанное ограничение не имеет места. В этом случае размер элементов, над которыми осуществляются вычисления при формировании и проверке подлинности ЭЦП, может быть существенно уменьшен, благодаря чему повышается вычислительная эффективность схем ЭЦП. Перспективными для такого применения являются нециклические группы известного порядка Ω при условии, что отношение Ω/Ω', где Ω' — максимальный порядок циклической подгруппы, является достаточно большим и значение Ω' делится на квадрат значения степени корня.

В данной работе рассматривается математическая задача построения нециклических групп, удовлетворяющих отмеченному выше условию, и криптографическое применение построенных групп в схемах ЭЦП, основанных на сложности задачи извлечения корней большой простой степени.

1. Построение нециклических конечных групп векторов

Рассмотрим множество векторов вида $(a, b) = a\mathbf{e} + b\mathbf{i}$, где $\mathbf{i}$ и $\mathbf{e}$ — базисные вектора; a и b – целые числа, принадлежащие конечному кольцу Z_m, называемые координатами. Выражения $a\mathbf{e}$ и $b\mathbf{i}$ обозначают вектора $(a, 0)$ и $(0, b)$ соответственно и называются компонентами вектора (a, b). Определим операцию сложения векторов как сложение одноименных координат: $(a, b) + (c, d) = (a + c, b + d)$, где знак + применен для обозначения двух разных операций — сложения элементов кольца Z_m и сложения векторов, что не вносит неопределенности ввиду очевидности его интерпретации в каждом случае его применения. Операцию умножения векторов $a\mathbf{e} + b\mathbf{i}$ и $c\mathbf{e} + d\mathbf{i}$ определим по правилу «умножения многочленов»: $(a\mathbf{e} + b\mathbf{i}) \circ (c\mathbf{e} + d\mathbf{i}) = ac\mathbf{e} \circ \mathbf{e} + bc\mathbf{i} \circ \mathbf{e} + ad\mathbf{e} \circ \mathbf{i} + bd\mathbf{i} \circ \mathbf{i}$, где операция умножения $\circ$ имеет более высокий приоритет по сравнению со сложением, а произведения пар базисных векторов заменяются базисным вектором или однокомпонентным вектором в соответствии со следующим правилом подстановки: $\mathbf{e} \circ \mathbf{e} = \mathbf{e}$; $\mathbf{i} \circ \mathbf{e} = \mathbf{e} \circ \mathbf{i} = \mathbf{i}$; $\mathbf{i} \circ \mathbf{i} = \varepsilon\mathbf{e}$. Координата ε называется коэффициентом растяжения, выбор которого задает тот или иной тип конечных групп двухмерных векторов. Таким образом, операция умножения векторов (a, b) и (c, d) выполняется по правилу:

$$(a, b)(c, d) = ((ac + \varepsilon bd) \bmod m, (ad + bc) \bmod m) = g'\mathbf{e} + h'\mathbf{i},$$

где $g' = (ac + \varepsilon bd) \bmod m$ и $h' = (ad + bc) \bmod m$. Легко проверить, что определенная операция умножения обладает свойствами ассоциативности и коммутативности, а нейтральным элементом по умножению является вектор $E = (1, 0)$. 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:

$$(a\mathbf{e} + b\mathbf{i})(x\mathbf{e} + y\mathbf{i}) = ((ax + \varepsilon by) \bmod m)\mathbf{e} + (ay + bx) \bmod m)\ \mathbf{i} = 1\mathbf{e} + 0\mathbf{i}.$$

Из последней записи вытекает, что для определения обратных значений необходимо решать следующую систему из двух линейных сравнений с двумя неизвестными:

$$ax + \varepsilon by \equiv 1 \mod m \ \text{ и } \ ay + bx \equiv 1 \mod m. \qquad (1)$$

Формирование конечных нециклических групп с требуемыми значениями порядка обеспечим выбором значения m, равного простому значению ρ (случай 1), и значения m, равного квадрату простого числа ρ (случай 2), при соответствующем выборе коэффициента ε.

Случай 1.

Утверждение 1. Пусть $m = \rho$, где ρ — нечетное простое число. При значении $\varepsilon > 1$, являющемся квадратичным невычетом по модулю ρ, формируется группа двухмерных векторов порядка $\Omega = (\rho - 1)^2$.

Доказательство. Приравнивая к нулю главный определитель системы (1), получаем характеристическое уравнение

$$a^2 - \varepsilon b^2 \equiv 0 \bmod \rho. \qquad (2)$$

Для каждого вектора (a, b), координаты которого удовлетворяют уравнению (2), не существует обратного вектора. Такими векторами являются (0, 0) и все вектора вида $(\varepsilon^{1/2}b \mod \rho, b)$ и $(-\varepsilon^{1/2}b \mod \rho, b)$, где $b \in \{1, \ldots, \rho-1\}$ и $\varepsilon^{1/2}$ — некоторое целое значение. Очевидно, что координаты всех других векторов не удовлетворяют уравнению (1), а следовательно, для них существуют обратные вектора. Число всех векторов, заданных над простым полем Z_ρ, равно ρ^2. Для $2(\rho-1)+1$ вектора нет обратных значений, поэтому все оставшиеся вектора образуют мультипликативную группу порядка

$$\Omega = \rho^2 - 2(\rho-1) - 1 = (\rho-1)^2.$$

Утверждение доказано.

Эксперимент [3] показывает, что группы, соответствующие условиям утверждения 1, являются нециклическими и максимальный порядок циклических подгрупп составляет $\Omega' = (\rho-1)$. Этот случай представляет для нас существенный интерес при следующей структуре простого числа $\rho = Nk^2 + 1$, где k – простое 160-битовое число и N – сравнительно малое четное число. В работе [4] показано, что доля простых чисел с такой структурой достаточно велика и они могут быть легко сформированы для значений $8 \le |k| \le 512$ бит и $2 \le |N| \le 8$ бит, где $|k|$ и $|N|$ обозначают размер чисел k и N.

Случай 2.

Утверждение 2. Пусть $m = \rho^2$, где ρ — нечетное простое число. При значении ε, таком, что $\rho \mid \varepsilon$, формируется группа двухмерных векторов порядка $\Omega = \rho^3(\rho-1)$.

Доказательство. При заданных условиях для элементов (a, b), таких, что a не делится на ρ, характеристическое уравнение (1) не имеет решений, поскольку $\rho \mid \varepsilon$, а определитель системы сравнений является взаимно простым с модулем ρ^2, т. е. для каждого из указанных элементов имеются обратные значения. При этом операция умножения двух элементов дает третий элемент, в котором первая координата также не делится на ρ, т. е. операция умножения является замкнутой на указанном множестве пар (a, b). Следовательно, это множество является группой, порядок которой можно определить из того факта, что число возможных значений первой координаты равно функции Эйлера от модуля $\varphi(\rho^2) = \rho(\rho-1)$, а число возможных значений второй координаты равно ρ^2. Получаем следующую формулу для значения порядка построенной мультипликативной группы:

$$\Omega = \rho(\rho-1)\cdot\rho^2 = \rho^3(\rho-1).$$

Утверждение доказано.

Согласно теореме Силова [5], в группах, соответствующих условиям утверждения 2, содержатся подгруппы порядка ρ, ρ^2 и ρ^3, причем известна теорема, что любая подгруппа простого порядка является циклической, т. е. в построенной группе существуют циклические группы порядка ρ. Однако нас интересуют нециклические группы, содержащие циклические подгруппы, порядок которых делится на квадрат простого числа. Поэтому важным является выяснение вопроса существования циклических подгрупп порядка ρ^2 и ρ^3. Ответ на этот вопрос был получен экспериментальным путем с помощью специально разработанной программы для ЭВМ. Опыт показал, что в построенной группе содержатся циклические подгруппы порядка

$$\Omega' = \rho^2(\rho-1),$$

что делает эти группы перспективными для решения нашей задачи синтеза алгоритмов ЭЦП, основанных на вычислительной сложности нахождения корней ρ-й степени и обеспечивающих повышение производительности по сравнению с алгоритмами, предложенными в работе [1]. Таблица 1 иллюстрирует экспериментальные результаты по исследованию строения групп для случаев 1 и 2. Приведем некоторые примеры групп, соответствующих рассмотренным случаям 1 и 2.

Примеры.

1. Пусть $m = \rho = 10301$ – простое число и $\varepsilon = 10002$ – квадратичный вычет по модулю 10301. Формируется нециклическая группа порядка $\Omega = (\rho-1)^2$. Элемент (17, 11) имеет порядок $\omega(17, 11) = 10300 = (\rho-1)$, который является максимально возможным в рассматриваемой группе.

Последнее означает, что циклических подгрупп, порядок которых превышает значение $\rho - 1$, не существует. Эксперимент показывает, что такая ситуация имеет место и для других значений простого числа ρ и квадратичного вычета $\varepsilon \pmod{\rho}$. Для построения алгоритмов ЭЦП, основанных на вычислительной сложности нахождения корней простой степени k, такой, что $k \mid \rho - 1$, требуется использовать значения ρ, для которых выполняется условие $k^2 \mid \rho - 1$, поскольку для обеспечения высокой сложности задачи извлечения корней требуется обеспечить условие делимости порядка циклических подгрупп на квадрат степени корня.

2. Пусть $m = \rho^2 = 10201$, где $\rho = 101$ – простое число и $\varepsilon = 101$. Формируется нециклическая группа порядка $\Omega = \rho^3(\rho - 1)$. Элемент (7, 11) является генератором циклической подгруппы порядка $\Omega' = \rho^2(\rho - 1) = 1020100$. Это является максимальным значением порядка по всем циклическим подгруппам. Элемент (1718, 7660) имеет порядок $\omega(1718, 7660) = 10201$ и является генератором циклической группы порядка $\rho^2 = 10201$.

2. Оценка сложности задачи извлечения корней в группах векторов

Оценка сложности задачи извлечения корней простой степени k в группах, соответствующих случаю 1 при $\rho = Nk^2 + 1$, и простой степени ρ в группах, соответствующих случаю 1, требует выбора наиболее эффективного известного алгоритма решения этой задачи. Из известных в литературе алгоритмов решения этой задачи в мультипликативной группе поля $GF(\rho)$ при $\rho = Nk^2 + 1$ наименьшую вычислительную сложность при $|k| < 160$ бит и $|\rho| > 1024$ бит имеет алгоритм непосредственного вычисления корней, предложенный в работе [2], а при $|k| > 160$ бит и $|\rho| < 1024$ бит алгоритм, включающий предварительное вычисление дискретного логарифма элемента, из которого вычисляется корень степени k [2]. Аналогичные алгоритмы вычисления корней могут быть построены и для рассматриваемых групп двухмерных векторов. Для этого полезно знать строение этих групп. Для общего случая векторов произвольной размерности, заданных над простыми полями, этот вопрос детально рассмотрен в работе [2], где показано, что конечные группы векторов характеризуются строением, описываемым в терминах многомерной цикличности.

Таблица 1. Строение частных вариантов построенных групп (N_ω – число элементов порядка ω)

Случай 1				Случай 2			
$p = 331$; $\varepsilon = 4$		$p = 281$; $\varepsilon = 25$		$p = 23$; $\varepsilon = 46$		$p = 29$; $\varepsilon = 58$	
ω	N_ω	ω	N_ω	ω	N_ω	ω	N_ω
2	3	2	3	2	1	2	1
3	8	4	12	11	10	7; 14	6
5	24	5	24	22	10	28	12
6	24	7	48	23	528	29	840
10	72	8	48	46	528	58	840
11	120	10	72	253	5280	116	1680
15	192	14	144	506	5280	203	5040
22	360	20	288	529	11638	406	5040
30	576	28	576	1058	11638	812	10080
33	960	35	1152	5819	116380	841	23548
55	2880	40	1152	11638	116380	1682	23548
66	2880	56	2304	Проверка: $1 + \sum N_\omega = 267674$ $p^3(p-1) = 267674$		3364	47096
110	8640	70	3456			5887	141288
165	23040	140	13824			11774	141288
330	69120	280	55296			23548	282576

Интерпретация полученных экспериментальных и теоретических результатов по построенным в разделе 2 группам двухмерных векторов в терминах многомерной цикличности и использование формул для определения количества элементов группы, имеющих заданное значение порядка, позволяют определить количество циклических подгрупп каждого возможного значения порядка. Кроме того, из результатов [2] следует, что рассматриваемые группы двухмерных векторов имеют двумерную цикличность и для каждого из случаев 1 и 2 группы все элементы группы могут быть порождены некоторыми парами элементов, например G_1 и G_2, как некоторые степени этих элементов. Таким образом, любой двухмерный вектор A, принадлежащий группе, может быть представлен в виде $A = G_1^i \circ G_2^j$, где i и j — целочисленные степени, причем $i, j < \Omega'$ (Ω' максимальный порядок циклической подгруппы).

Предположим, что для элемента Y уравнение $X = \sqrt[k]{Y}$ (случай 1) или уравнение $X = \sqrt[p]{Y}$ (случай 2) имеет решение. Рассмотрим для определенности случай 2. Пусть решением является некоторый вектор $X = G_1^{i_x} \circ G_2^{j_x}$. Поскольку $X^p = \left(G_1^{i_x} \circ G_2^{j_x}\right)^p = G_1^{pi_x} \circ G_2^{pj_x} = Y$, то вычисление корня можно свести к вычислению дискретного логарифма по двухмерному основанию (G_1, G_2). Решение последней задачи даст значение двухмерного логарифма от Y, равное $(i_y, j_y) = (pi_x, pj_x)$, из которого легко найти (i_x, j_x) и $X = G_1^{i_x} \circ G_2^{j_x} = \sqrt[p]{Y}$. Рассмотрим следующий алгоритм вычисления двухмерного логарифма и оценим его трудоемкость.

1. Вычислить значения $Y \circ G_1^{-i}$ для всех $i < \Omega'$ и запомнить их в некотором массиве M1 (трудоемкость этого шага W_1 примерно равна Ω' операций возведения в степень).

2. Упорядочить массив M1 по значениям $Y \circ G_1^{-i}$ ($W_2 \approx \Omega' \log_2 \Omega'$ операций сравнения).

3. Последовательно для $j = 0,1,2\ldots$, Ω' вычислить G_2^j и проверить, имеется ли такое значение в массиве M1, пока для некоторого j_0 не будет получено $G_2^{j_0}$, присутствующее в M1 и соответствующее некоторому i_0 (W_3 не превышает $\Omega' \log_2 \Omega'$ операций сравнения и Ω' операций возведения в степень).

После завершения работы алгоритма имеем $Y = G_1^{i_0} \circ G_2^{j_0}$ и $X = G_1^{\frac{i_0}{p}} \circ G_2^{\frac{j_0}{p}}$. В целом трудоемкость этого алгоритма можно оценить как $O(\Omega')$ операций возведения в степень (операции сравнения имеют меньшую сложность). Легко свести задачу нахождения «двухмерного» логарифма в исходной группе к задаче нахождения «двухмерного» логарифма в подгруппе порядка ρ^2, имеющей двухмерное циклическое строение. В последнем случае рассмотренный алгоритм имеет трудоемкость $W = O(q)$, где q — максимальный простой делитель Ω', т. е. $q = k$ в случае 1 и $q = \rho$ в случае 2.

Рассмотрим алгоритм непосредственного вычисления корня ρ-й степени в случае 2. Легко видеть, что $X^{\Omega'} = Y^{\Omega'/\rho} = E$, где E — единичный вектор, поэтому имеем $Y^{\Omega'/\rho} = E^{1/\rho}$. В рассматриваемой группе содержится подгруппа Γ_2 порядка ρ^2, все элементы которой, кроме единичного, имеют порядок ρ и являются корнями ρ-й степени из единичного элемента. Два случайно выбранных элемента G_{E1} и G_{E2} порядка ρ (их можно найти по способу, описанному в [7. С. 20—21]) с вероятностью, близкой к 1, будут принадлежать различным подгруппам и составят двумерный генератор подгруппы Γ_2. При некоторых степенях i и j выполняется $Y^{\frac{\Omega'}{\rho^2}} = G_{E1}^i \circ G_{E2}^j$. Это соотношение лежит в основе следующего алгоритма.

1. Вычислить значения $Y^{\frac{\Omega'}{\rho^2}} \circ G_{E1}^{-i}$ для всех $i < \rho$ и запомнить их в некотором массиве M1 (трудоемкость этого шага W_1 примерно равна ρ операций возведения в степень).

2. Упорядочить массив M1 по значениям $Y^{\frac{\Omega'}{\rho^2}} \circ G_{E1}^{-i}$ ($W_2 \approx p \log_2 p$ операций сравнения).

3. Последовательно для $j = 0,1,2\ldots$, ρ вычислить G_{E2}^j и проверить, имеется ли такое значение в массиве M1, пока для некоторого j_0 не будет получено $G_{E2}^{j_0}$, присутствующее в M1 и как значение $Y^{\frac{\Omega'}{\rho^2}} \circ G_{E1}^{-i_0}$, соответствующее показателю i_0 ($W_3 \le p \log_2 p$ операций сравнения и ρ операций возведения в степень).

В целом трудоемкость этого алгоритма равна $O(p)$ операций возведения в степень. Рассмотренный алгоритм применим также для нахождения корней степени k в случае 1, при этом его трудоемкость равна $O(k)$. При значениях $|\rho| \geq 80$ бит (для случая 2) и $|k| \geq 80$ бит (для случая 2) нахождение корней простых степеней ρ и k в рассматриваемых нециклических группах вычислительно невыполнимо, поскольку это требует выполнения более 2^{80} операций возведения в степень.

3. Алгоритм электронной цифровой подписи

Группы, относящиеся к рассмотренным выше случаям 1 и 2, могут быть использованы для построения алгоритмов ЭЦП, основанных на сложности задачи нахождения корней большой простой степени k в нециклических конечных группах. В первом случае следует использовать такое простое число ρ, что $k^2 \mid \rho - 1$, где размер значения $|k|$ ≥ 80 бит. Во втором случае в качестве степени выбирается значение ρ, такое, что $|\rho|$ ≥ 80 бит, и на структуру выбираемого простого модуля ограничений не накладывается. Указанные размеры параметров k и ρ обеспечиваются выбором размера модуля $|\rho| \geq 160$ бит и модуля $|\rho^2| \geq 160$ бит соответственно в случаях 1 и 2.

Рассмотрим построение алгоритма ЭЦП в случае 1. В качестве секретного ключа используется элемент X группы Г порядка Ω, такой, что $\omega(X) \geq k^2$. Открытый ключ генерируется по формуле $Y = X^k$. Процедура генерации ЭЦП состоит в следующем.

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

2. Вычисляется значение $R = T^k$.

3. Вычисляется значение хэш-функции F_H от подписываемого документа M, к которому предварительно присоединяются координаты r_1 и r_2 элемента R: $E = F_H(M\|r_1\|r_2)$, где $\|$ – операция конкатенации. Значение E является первым элементом ЭЦП.

4. Вычисляется второй элемент ЭЦП: $S = T \cdot X^E$.

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

1. Вычисляется значение $R' = Y^{\Omega - E} S^k$.

2. Вычисляется значение хэш-функции $E' = F_H(M\|r'_1\|r'_2)$, где r'_1 и r'_2 – координаты элемента $R' \in$ Г.

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

Аналогично можно реализовать алгоритмы ЭЦП и на группах, относящихся к случаю 2 из раздела 2 (с заменой во всех формулах величины k на величину ρ; например, открытый ключ будет вычисляться по формуле $Y = X^\rho$). Стойкость таких алгоритмов ЭЦП определяется сложностью задачи извлечения корней, рассмотренной в разделе 3.

4. Сопоставление с известными алгоритмами

В приводимой ниже таблице 2 представлена сравнительная оценка производительности различных алгоритмов ЭЦП в случае уровня безопасности, равного 2^{80} операций возведения в степень.

Таблица 2. Сравнение производительности алгоритмов ЭЦП

Алгоритм ЭЦП	Размер ЭЦП	Размер ОК	Произв., отн. ед.
ГОСТ Р 34.10-94	320*	1024	1
ГОСТ Р 34.10-2001	320*	320*	2,5
ECDSA	320	320	2,5
Предложенный ($\|k\| \approx 80$ бит)	400	320	16
Предложенный ($\|k\| \approx 160$ бит)**	800	640	4

* В спецификации стандартов рекомендуются размеры значений ЭЦП и открытого ключа (ОК), превышающие 320 бит;
** Соответствует уровню безопасности 2^{160} операций возведения в степень.

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, а предложенный — на 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 двухмерных векторов, координатами которых являются элементы кольца вычетов по модулю, равному простому числу или квадрату простого числа. Представлена схема ЭЦП, обладающая существенно более высокой производительностью по сравнению с известными алгоритмами ЭЦП.

СПИСОК ЛИТЕРАТУРЫ:

1. *Молдовян Н. А.* Извлечение корней по простому модулю как криптографический примитив // Вестник СПбГУ. Сер. 10. 2008. Вып. 1. С. 100–105.
2. *Молдовян А. А., Молдовян Н. А.* Новые алгоритмы и протоколы для аутентификации информации в АСУ // Автоматика и телемеханика. 2008. № 7. С. 157–169.
3. *Молдовян Н. А.* Группы векторов для алгоритмов электронной цифровой подписи // Вестник СПбГУ. Сер. 10. 2009 (в печати).
4. *Moldovyan N. A.* Digital Signature Scheme Based on a New Hard Problem // Computer Science Journal of Moldova. 2008. Vol. 16. № 2 (47). P. 163–182.
5. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. М.: Физматлит, 1996. – 287 с.
6. *Молдовян Н. А.* Многомерная цикличность групп векторов и их использование в алгоритмах аутентификации информации // Вестник СПбГУ. Сер. 10. 2009 (в печати).
7. *Молдовян Н. А.* Практикум по криптосистемам с открытым ключом. СПб.: БХВ – Петербург, 2007. – 298 с.