Е. С. Дернова, А. А. Костина, Н. А. Молдовян, П. А. Молдовяну

ЗАДАНИЕ ВЕКТОРНЫХ КОНЕЧНЫХ ПОЛЕЙ И ГРУПП В СЛУЧАЕ ПРОИЗВОЛЬНОЙ РАЗМЕРНОСТИ[1]

Введение

Механизмы электронной цифровой подписи (ЭЦП) играют важную роль в современных информационных технологиях для придания юридической силы электронным документам [1, 2]. В ряде случаев применения ЭЦП требуется обеспечение высокой производительности механизмов аутентификации электронных сообщений, что обусловливает интерес к поиску новых криптографических примитивов, ориентированных на увеличение быстродействия и снижение стоимости аппаратной реализации. Значительным достижением явилось использование эллиптических кривых (ЭК), заданных над конечными полями, для построения алгоритмов ЭЦП [3–5]. В работе [6] с целью дальнейшего увеличения производительности алгоритмов ЭЦП предложено использовать для их синтеза векторные конечные поля и векторные конечные группы. Однако применение ВКП и векторных конечных групп в качестве базового примитива алгоритмов ЭЦП связано с длительным предварительным исследованием сложности задачи дискретного логарифмирования в таких структурах. Этот вопрос снимается в случае применения ВКП в качестве базовых полей, над которыми задаются ЭК, применяемые в качестве криптографического примитива. В силу изоморфизма всех конечных полей заданного порядка свойства ЭК будут определяться характеристикой и степенью расширения конечного поля, над которым определяется ЭК, и будут независимы от формы задания поля.

Перенос алгоритмов эллиптической криптографии на ВКП обеспечивает существенное повышение их производительности за счет 1) снижения сложности операции умножения в поле при заданном размере порядка поля (под размером некоторой величины здесь и далее понимается ее разрядность в двоичном представлении) и 2) за счет возможности эффективного распараллеливания операции умножения в поле. Умножение векторов в ВКП производится с использованием специальных таблиц, определяющих результат умножения базисных векторов. Эти таблицы называются таблицами умножения базисных векторов. Необходимым условием формирования ВКП является использование в ТУБВ специально выбираемых коэффициентов растяжения.

Группы векторов представляют отдельный интерес для построения скоростных алгоритмов ЭЦП. В общем случае они описываются в терминах многомерной цикличности. Частным случаем являются циклические группы векторов. Этот случай соответствует формированию ВКП. При заданном значении размерности m векторов размерность цикличности групп векторов равна

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

μ, где $1 \le \mu \le m$. При этом конкретное значение μ определяется распределением и значениями коэффициентов растяжения, а также характеристикой поля, над которым заданы вектора. Подробно строение групп векторов и варианты их использования для построения схем ЭЦП рассмотрены в статье [7].

В настоящей работе рассматривается вопрос снижения сложности операции умножения векторов в ВКП и группах векторов, а также схема построения алгоритмов ЭЦП на основе групп векторов, обладающих многомерной цикличностью строения.

1. Конечные векторные поля

Рассмотрим конечные множества m-мерных, которые представляются в виде $(a,b,\ldots,q)$ или виде $a\mathbf{e} + b\mathbf{i} + \ldots + q\mathbf{w}$, где $\mathbf{e}$, $\mathbf{i}$, …, $\mathbf{w}$ — формальные базисные вектора и $a,b,\ldots,q \in GF(\rho^s)$ — координаты вектора, являющиеся элементами конечного поля $GF(\rho^s)$, где ρ — простое число, называемое характеристикой поля, и $s \ge 1$ — степень расширения поля. Сложение векторов определяется по формуле:

$$(a,b,\ldots,q) + (x,y,\ldots,z) = (a + x, b + y, \ldots, q + z).$$

Одноразмерные вектора вида $\varepsilon\mathbf{v}$, где $\varepsilon \in GF(\rho^s)$ и $\mathbf{v}$ — некоторый формальный базисный вектор, входящие во вторую форму записи векторов и разделенные знаком суммы, представляют собой компоненты вектора. Операция умножения векторов определяется по естественному правилу попарного перемножения всех компонентов по формуле:

$$(a\mathbf{e} + b\mathbf{i} + \ldots + q\mathbf{w})\circ(x\mathbf{e} + y\mathbf{i} + \ldots + z\mathbf{w}) = ax\mathbf{e}\circ\mathbf{e} + ay\mathbf{e}\circ\mathbf{i} + \ldots$$
$$+ az\mathbf{e}\circ\mathbf{w} + \ldots + bx\mathbf{i}\circ\mathbf{e} + by\mathbf{i}\circ\mathbf{i} + \ldots + bz\mathbf{i}\circ\mathbf{w} + \ldots + qx\mathbf{j}\circ\mathbf{e} + qy\mathbf{w}\circ\mathbf{i} + \ldots + qz\mathbf{w}\circ\mathbf{w},$$

в которой вместо каждого из произведений двух базисных векторов подставляется однокомпонентный вектор, определяемый по ТУБВ. Координата этого однокомпонентного вектора называется коэффициентом растяжения и указывается в соответствующих клетках ТУБВ. Совокупность клеток ТУБВ, в которых присутствует один и тот же коэффициент растяжения, определяет тип распределения этого коэффициента. В случае, когда определенное с помощью ТУБВ векторное умножение является коммутативной и ассоциативной операцией, КМВ является конечным векторным кольцом. При этом мультипликативная группа кольца генерируется некоторым набором из μ векторов $Z_1, Z_1,\ldots, Z_\mu$, где $\mu \mid m$. Любой вектор из этой группы представим в виде произведения некоторых степеней элементов $Z_1, Z_1,\ldots, Z_\mu$. Такое строение интерпретируется как μ-мерная цикличность [7]. Конкретное значение μ определяется значением m, распределением базисных векторов в ТУБВ, распределением коэффициентов растяжения в ТУБВ и значением этих коэффициентов. Особый интерес представляет случай одномерной цикличности, при реализации которой образуются ВКП. В работе [6] показано, что ВКП формируются при следующих условиях:

- размерность векторного пространства является делителем числа $\rho^s - 1$, т. е. $m \mid \rho^s - 1$;
- задание операции умножения векторов с помощью ТУБВ, обеспечивающей свойства коммутативности и ассоциативности умножения векторов;
- наличие в ТУБВ коэффициентов растяжения, которые не могут быть представлены в виде d-й степени какого-либо элемента базового поля $GF(\rho^s)$, где $s \ge 2$, d — нетривиальный делитель размерности m.

Построение таблиц умножения базисных векторов с требуемыми свойствами выполняется в два этапа. Сначала строится исходная таблица без коэффициентов растяжения (см. распределение базисных векторов в таблице 1), а затем в нее вносятся коэффициенты, распределяемые таким образом, что обеспечивается ассоциативность и коммутативность умножения векторов. Существует два общих типа распределения коэффициентов растяжения, обеспечивающих формирование конечных векторных полей [8] для произвольных значений m, которые будем называть

стандартными распределениями коэффициентов растяжения. Эти распределения представлены в таблице 1 как распределения коэффициентов ε и μ.

Таблица 1. Стандартные распределения независимых растягивающих коэффициентов ε и μ для произвольных значений m

∘	***e***	***i***	***j***	***k***	***u***	***v***	...	...	***z***
e	**e**	**i**	**j**	**k**	**u**	**v**	...	...	**z**
i	**i**	ε**j**	ε**k**	ε**u**	ε**v**	ε...	ε...	ε**z**	με**e**
j	**j**	ε**k**	ε**u**	ε**v**	ε...	ε...	ε**z**	με**e**	μ**i**
k	**k**	ε**u**	ε**v**	ε...	ε...	ε**z**	με**e**	μ**i**	μ**j**
u	**u**	ε**v**	ε...	ε...	ε**z**	με**e**	μ**i**	μ**j**	μ**k**
v	**v**	ε...	ε...	ε**z**	με**e**	μ**i**	μ**j**	μ**k**	μ**u**
...	...	ε...	ε**z**	με**e**	μ**i**	μ**j**	μ**k**	μ**u**	μ**v**
...	...	ε**z**	με**e**	μ**i**	μ**j**	μ**k**	μ**u**	μ**v**	μ...
z	**z**	με**e**	μ**i**	μ**j**	μ**k**	μ**u**	μ**v**	μ...	μ...

Обозначим базисные вектора **e**, **j**, **k**, **u**, **v**… как $\mathbf{v}_0$, $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$, $\mathbf{v}_4$… соответственно. Покажем, что при $\varepsilon = 1$ при любом значении $\mu \in GF(\rho^s)$, где $s \geq 1$, для произвольных троек $\mathbf{v}_i$, $\mathbf{v}_j$ и $\mathbf{v}_k$, где i, j, $k \in \{0,1,2,\ldots,m-1\}$, выполняется закон ассоциативности умножения базисных векторов:

$$(\mathbf{v}_i \circ \mathbf{v}_j) \circ \mathbf{v}_k = \mathbf{v}_i \circ (\mathbf{v}_j \circ \mathbf{v}_k). \quad (1)$$

Легко заметить, что для любых пар значений i и j имеет место

$$\mathbf{v}_i \circ \mathbf{v}_j = \mu^b \mathbf{v}_h, \quad (2)$$

где $h = (i + j) \bmod m$ и $b = (i + j) \operatorname{div} m$. Аналогично для любых троек $i, j, k \in \{0,1,2,\ldots,m-1\}$ имеет место

$$\mathbf{v}_i \circ \mathbf{v}_j \circ \mathbf{v}_k = \mu^b \mathbf{v}_h, \quad (3)$$

где $h = (i + j + k) \bmod m$ и $b = (i + j + k) \operatorname{div} m$. Из (3) непосредственно следует справедливость соотношения (1). Из описанного правила умножения векторов и ассоциативности и коммутативности умножения базисных векторов при $\varepsilon = 1$ и любом значении $\mu \in GF(\rho^s)$ следует, что второй тип распределения коэффициентов растяжения обеспечивает свойства коммутативности и ассоциативности умножения векторов. Аналогично доказывается, что и первый тип распределения коэффициентов растяжения обеспечивает эти свойства. Легко показать, что если найдены несколько распределений коэффициентов растяжения для некоторой данной исходной ТУБВ, обеспечивающие свойства коммутативности и ассоциативности умножения, то их суперпозиция также обеспечивает эти свойства. Для типовой исходной ТУБВ при простых значениях m экспериментально установлено существование $m - 1$ различных распределений коэффициентов растяжения, в каждом из которых растягивающий коэффициент вносится в $m(m-1)/2$ клеток ТУБВ. Такие распределения для различных частных значений размерности приведены в работе [8]. В случае произвольных четных значений m найдено распределение, в котором заполняются только $m^2/4$ клеток ТУБВ. Данное распределение описывается в следующем разделе.

2. Распределение растягивающих коэффициентов при четной размерности

Каждая клетка ТУБВ, содержащая отличный от единицы коэффициент, определяет дополнительную операцию умножения в базовом поле $GF(\rho^s)$, которую надо выполнить при осуществлении умножения двух векторов. Поэтому целесообразно построить ТУБВ со сравнительно малым числом клеток, заполняемых коэффициентом растяжения. В случае четных размерностей сюда относится распределение, в котором заполняется клетка, расположенная во втором столбце и второй строке исходной ТУБВ, а также все остальные клетки, расположенные в четном столбце и четной строке.

Здесь предполагается, что столбцы (строки) нумеруются со столбца (строки), в верхней (первой) клетке которого (которой) расположен базисный вектор **e**. Данный тип распределения представлен в таблице 2. Покажем, что при любом значении $\varepsilon \in GF(\rho^s)$, где $s \geq 1$, для произвольных троек базисных векторов выполняется закон ассоциативности умножения базисных. Обозначим базисные вектора **e**, **j**, **k**, **u**, **v**… как $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$, $\mathbf{v}_4$, $\mathbf{v}_5$… соответственно. Пусть **[odd]** — базисный вектор с нечетным индексом, а **[even]** — базисный вектор с четным индексом.

Таблица 2. Распределение коэффициента растяжения случая четных значений m

∘	***e***	***i***	***j***	***k***	***u***	***v***	...	***t***
e	**e**	**i**	**j**	**k**	**u**	**v**	...	**t**
i	**i**	**εj**	**k**	**εu**	**v**	**ε...**	**t**	**εe**
j	**j**	**k**	**u**	**v**	...	**t**	**e**	**i**
k	**k**	**εu**	**v**	**ε...**	**t**	**εe**	**i**	**εj**
u	**u**	**v**	...	**t**	**e**	**i**	**j**	**k**
v	**v**	**ε...**	**t**	**εe**	**i**	**εj**	**k**	**εu**
...	...	**t**	**e**	**i**	**j**	**k**	**u**	**v**
t	**t**	**εe**	**i**	**εj**	**k**	**εu**	**v**	**ε...**

Из таблицы 2 легко заметить, что для любых конкретных пар базисных векторов всегда выполняется следующее правило: при перемножении базисных векторов различной четности результатом является четный базисный вектор **[even]**, при перемножении нечетных базисных векторов результатом является нечетный базисный вектор **[odd]**, а в случае перемножения двух четных базисных векторов результатом является вектор ε**[odd]**, т. е. растянутый в ε раз нечетный базисный вектор. Согласно этому правилу можно записать: **[odd]**∘**[even]** = **[even]**∘**[odd]** = **[even]**, **[odd]**∘**[odd]** = **[odd]** и **[even]**∘**[even]** = ε**[odd]**. Из последних формул непосредственная проверка показывает, что для произведений всех возможных троек базисных векторов выполняется свойство ассоциативности умножения указанных «обобщенных» базисных векторов, т. е. для произведений из произвольных троек обобщенных базисных векторов закон ассоциативности выполняется. Из этого вытекает, что введение коэффициентов растяжения по схеме, представленной в таблице 2, не нарушает ассоциативности умножения базисных векторов **e**, **j**, **k**, **u**, …, **t** .

Экспериментально установлено, что тип распределения, представляемый таблицей 2, задает формирование групп векторов μ-мерной цикличности, где $\mu = m$ или $\mu = m/2$. Векторные поля образуются только в случае $m = 2$ при соответствующем выборе значений коэффициентов растяжения. Для четных значений размерности $m \geq 4$ для формирования ВКП следует воспользоваться распределениями коэффициентов растяжения, задаваемыми таблицей 1. Для снижения сложности векторного умножения следует выбирать коэффициенты растяжения, имеющие минимально возможный размер (несколько битов).

3. Примеры векторных конечных полей и групп

Рассмотрим конкретные случаи формирования конечных полей в конечных векторных пространствах. В случае задания умножения векторов по ТУБВ, являющихся частными вариантами таблицы 1, соответствующих конкретным значениям размерности векторов, имеем следующие примеры.

Случай 1. ($m = 3$, $\rho = 127$ и $s = 5$). Рассмотрим пространство трехмерных векторов $a\mathbf{e} + b\mathbf{i} + c\mathbf{j}$, где координаты a, b и c представляют собой элементы поля многочленов $GF(127^5)$, причем умножение в этом поле задано по модулю неприводимого многочлена $\eta(z) = z^5 + 120z^4 + 16z^3 + 114z^2 + 69z + 34$. Определим операцию умножения трехмерных векторов с помощью таблицы 1 для случая $m = 3$ при следующих значениях коэффициентов растяжения

$\varepsilon = \varepsilon(z) = z^2 + 5z + 2$ и $\mu = 1$. Выбранные параметры и операция умножения векторов задают формирование векторного конечного поля $GF((127^5)^3)$.

Случай 2. ($m = 3$, $\rho = 2$ и $s = 16$). Рассмотрим конечное пространство трехмерных векторов $a\mathbf{e} + b\mathbf{i} + c\mathbf{j}$, где координаты a, b и c представляют собой двоичные многочлены поля $GF(2^{16})$. Пусть в поле многочленов $GF(2^{16})$ умножение задано по модулю неприводимого многочлена $\eta(z) = z^{16} + z^{15} + z^{14} + z^{12} + z^{11} + z^{10} + z^9 + z^2 + 1$, который можно также представить в виде $\eta(z) = (11101111000000101)$. Операцию умножения в векторном пространстве определим по таблице 1 для случая $m = 3$ при $\varepsilon = \varepsilon(z) = z^3 + 1$ и $\mu = 1$. Заданный вариант умножения векторов и выбранные параметры задают векторное конечное поле $GF((2^{16})^3)$, генератором мультипликативной группы которого является вектор $G = (1101)\mathbf{e} + (1001)\mathbf{i} + (110)\mathbf{j}$.

Случай 3. ($m = 6$, $\rho = 3112656501667$ и $s = 1$). Определим операцию умножения шестимерных векторов $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} + h\mathbf{u} + l\mathbf{u}$, где координаты a, b, c, d, h и l представляют собой числа, принадлежащие полю $GF(3112656501667)$, с помощью таблицы 1 при коэффициентах растяжения $\varepsilon = 322954349912431981009351 9$ и $\mu = 1$. Выбранные параметры задают формирование конечной группы векторов, обладающей r-мерной цикличностью и значением порядка $\Omega = (\rho^3 - 1)^r$, где $r = 2$ — размерность циклического строения группы. Данная группа векторов содержит подгруппу Γ' порядка $\Omega' = q^2$, которая включает большое число подгрупп простого порядка $q = 322954349912431981009351 9$, причем подгруппа Γ' не содержит подгрупп другого порядка, за исключением примитивной подгруппы, состоящей из одного единичного вектора. Все элементы подгруппы порядка $\Omega' = q^2$ генерируются как произведения всех возможных степеней некоторой пары векторов, составляющих систему образующих этой подгруппы. Например, рассматриваемая подгруппа Γ' генерируется следующей парой векторов:

$G_1 = (2461700031734, 482034324490, 156834270570, 1324447431161, 2740416991343, 1220868764310)$

и

$G_2 = (2538171306005, 283399862632, 192519072375, 891592729264, 760409728893, 2653262071023)$.

Рассмотрим частные случаи формирования конечных групп векторов при задании векторного умножения по таблице 2.

Случай 4. ($m = 6$, $\rho = 3112656501667$ и $s = 1$). Определим операцию умножения шестимерных векторов $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} + h\mathbf{u} + l\mathbf{u}$, где координаты a, b, c, d, h и l представляют собой числа, принадлежащие полю $GF(3112656501667)$, с помощью таблицы 2 при коэффициенте растяжения $\varepsilon = 2$. Выбранные параметры задают формирование конечной группы векторов, обладающей r-мерной цикличностью и значением порядка $\Omega = (\rho^2 - 1)^r$, где $r = 3$.

Случай 5. ($m = 6$, $\rho = 3112656501667$ и $s = 1$). Определим операцию умножения шестимерных векторов $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} + h\mathbf{u} + l\mathbf{u}$, где координаты a, b, c, d, h и l представляют собой числа, принадлежащие полю $GF(3112656501667)$, с помощью таблицы 2 при коэффициенте растяжения $\varepsilon = 4$. Выбранные параметры задают формирование конечной группы векторов, обладающей r-мерной цикличностью и значением порядка $\Omega = (\rho - 1)^r$, где $r = 6$.

4. Схемы ЭЦП на основе групп с многомерной цикличностью

Группы векторов в общем случае не являются циклическими, поэтому вопрос о дискретном логарифмировании в них в классической постановке не стоит. Действительно, в классической постановке этой задачи предполагается цикличность (т. е. одномерная цикличность в терминах многомерной цикличности) конечной группы, в которой рассматривается задача дискретного логарифмирования. Однако для того, чтобы воспользоваться этой особенностью строения групп векторов, следует изменить схему формирования открытого ключа. В стандартной схеме

задается циклическая подгруппа порядка $\Omega(G)$, которая содержит открытый ключ как один из элементов. Многомерная цикличность групп векторов предоставляет следующую положительную возможность. Открытый ключ Y может быть вычислен таким образом, что не будет известен второй элемент порядка $\Omega(Y)$, принадлежащий той же подгруппе, которой принадлежит и элемент Y. Для этого открытый ключ следует вычислять по формуле $Y = G_1^{x_1} \circ G_2^{x_2} \circ \ldots \circ G_r^{x_r}$, где $\Omega(G_i) = q$ для всех $i \in \{1,2,\ldots, r\}$ и вектора G_1, G_2, …, G_r составляют базис подгруппы порядка q^r, позволяющий выразить любой элемент порядка q группы векторов, обладающей r-мерной цикличностью. Секретным ключом является набор целых чисел x_1, x_2, …, x_r, каждое из которых не превышает значение $q - 1$. Вычисление секретного ключа по открытому связано с решением задачи дискретного логарифмирования по многомерному основанию G_1, G_2, …, G_r. При этом вычисление всех элементов секретного ключа должно осуществляться одновременно, т. е. вычислить секретный ключ по частям нельзя. Для нахождения подобного многомерного логарифма можно применить методы, подобные общим методам дискретного логарифмирования в конечных циклических группах [9]. Вычислительная сложность таких методов решения задачи дискретного логарифмирования по r-мерному основанию оценивается как $O\left(\sqrt{q^r}\right)$ операций возведения в степень. Из этой оценки следует, что минимальный уровень криптографической стойкости обеспечивается при $|q| \geq 160/r$ бит.

Рассмотрим построение алгоритма ЭЦП на основе группы векторов, описанной в предыдущем разделе как *случай* 3 ($m = 6$, $\rho = 3112656501667$ и $s = 1$). В этой группе векторов порядка $\Omega = (\rho^3 - 1)^r$, где $r = 2$, содержится подгруппа порядка $\Omega' = q^r$, $q = 3229543499124319810093519$ — простое число, обладающая многомерным циклическим строением и включающая $q + 1$ подгрупп порядка q. Сгенерированные по случайному закону вектора G_1 и G_2 (см. указанный случай), являющиеся генераторами подгрупп порядка q, с пренебрежимо малой вероятностью $(q + 1)^{-1}$ попадают в одну и ту же подгруппу порядка q. Поэтому с вероятностью, очень близкой к 1, они составляют двумерный генератор подгруппы порядка $\Omega' = q^r$, значит, формирование открытого ключа в виде пары шестимерных векторов Y_1 и Y_2 зададим по формулам $Y_1 = G_1^{x_1} \circ G_2^{x_2}$ и $Y_2 = G_1^{x_1 x_2} \circ G_2^{x_2^2 + x_1^2}$, где x_1 и x_2 — 80-битовые числа, составляющие секретный ключ. Проверочное уравнение зададим в виде

$$R = Y_1^{-e_1} \circ Y_2^{-e_2} \circ G_1^{s_1} \circ G_2^{s_2},$$

где числа e_1, e_2, s_1 и s_2, имеющие размер $|q|$ бит, являются элементами ЭЦП.

Процедура генерации подписи к сообщению M выполняется следующим образом.

1. Выбрать случайные 80-битовые значения t_1 и t_2 и вычислить вектор $R = (r_1, r_2) = G_1^{t_1} \circ G_2^{t_2}$.

2. Используя некоторую специфицированную 160-битовую хэш-функцию F_H, вычислить значение e, интерпретируемое как конкатенация двух 80-битовых чисел e_1 и e_2:

$$e = e_1 \| e_2 = F_H (M \| r_1 \| r_2).$$

3. Вычислить значения s_1 и s_2 по формулам

$$s_1 = t_1 + x_1 e_1 + x_1 x_2 e_2 \bmod q \text{ и } s_2 = t_2 + x_2 e_1 + (x_1^2 + x_2^2) e_2 \bmod q.$$

Подписью является четверка чисел e_1, e_2, s_1 и s_2, общий размер которой равен примерно 320 бит.

Процедура проверки ЭЦП состоит в выполнении следующих шагов:

1. Вычислить вектор $R' = (r_1' \| r_2') = Y_1^{-e_1} \circ Y_2^{-e_2} \circ G_1^{s_1} \circ G_2^{s_2}$ и значение $e' = e_1' \| e_2' = F_H (M \| r_1' \| r_2')$.

2. Сравнить значения e и e'. Если $e_1' \| e_2' = e_1 \| e_2$, то подпись принимается.

Заключение

Показано, что для всех значений размерности векторов, заданных над конечным полем $GF(\rho^s)$, где $s \geq 3$, ВКП образуются при использовании ТУБВ вида, задаваемого таблицей 1. Для уменьшения сложности умножения в ВКП следует выбирать коэффициенты растяжения,

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.