УДК 681.3

ГОМОМОРФИЗМ КОНЕЧНЫХ ГРУПП ВЕКТОРОВ МАЛОЙ РАЗМЕРНОСТИ И СИНТЕЗ СХЕМ ЦИФРОВОЙ ПОДПИСИ

П. А. Молдовяну,
канд. техн. наук, начальник службы главного метролога
Н. А. Молдовян,
доктор техн. наук, главный научный сотрудник
ФГУП НИИ «Вектор»
Е. С. Дернова,
аспирант
А. А. Костина,
аспирант
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

Описывается гомоморфное отображение мультипликативной конечной группы векторов в мультипликативную группу конечного поля, над которым они заданы. Установленный гомоморфизм имеет значение для криптоанализа алгоритмов электронной цифровой подписи на основе сложности задачи дискретного логарифмирования в циклических подгруппах нециклической группы векторов. Предложен алгоритм электронной цифровой подписи, в котором учитывается наличие установленного гомоморфизма.

Ключевые слова *— векторное пространство, гомоморфизм, конечные группы, многомерная цикличность, цифровая подпись.*

Введение

В качестве криптографического примитива алгоритмов электронной цифровой подписи (ЭЦП) недавно были предложены векторные конечные поля (ВКП) и векторные конечные группы, задаваемые в конечных векторных пространствах в зависимости от типа определяемой операции умножения векторов [1]. В частности, схемы ЭЦП, обладающие достаточно высокой производительностью, разработаны на основе сложности задачи извлечения корней в конечных нециклических группах двухмерных векторов [2], а векторные конечные поля перспективны для задания на их основе эллиптических кривых, что позволяет значительно ускорить алгоритмы эллиптической криптографии за счет возможности распараллеливания операции умножения в базовом поле [1]. Мультипликативные группы векторов в общем случае являются нециклическими, однако они имеют характерное строение, которое можно описать в терминах многомерной цикличности [3]. Это понятие включает в себя и циклическое строение конечных групп как случай одномерной цикличности. Размерность цикличности строения некоторой группы векторов определяется типом задаваемой операции умножения векторов. Случаи формирования групп с одномерной цикличностью соответствуют заданию векторных конечных полей [3].

Построение алгоритмов ЭЦП на основе использования групп с многомерной цикличностью и их особенности представлены в работе [3]. Однако такие конструкции являются новыми и требуют выполнения значительных работ по их криптоанализу, т. е. исследованию стойкости ко всевозможным типам атак. Частные виды криптоанализа основываются на поиске гомоморфизмов.

В данной работе описывается достаточно общий гомоморфизм мультипликативной конечной группы векторов в мультипликативную группу конечного поля, над которым задано векторное пространство. Данное гомоморфное отображение и связанные с ним потенциальные атаки учтены в построенной схеме ЭЦП, использующей многомерность циклического строения групп векторов.

Многомерная цикличность строения конечных групп векторов

Рассмотрим конечные множества m-мерных векторов над конечным полем, которые представляются в виде $(a, b, ..., q)$ или в виде $a\mathbf{e} + b\mathbf{i} + ... + q\mathbf{w}$, где $\mathbf{e}, \mathbf{i}, ..., \mathbf{w}$ — формальные базисные векторы и $a, b, ..., q \in GF(p^s)$ — координаты вектора, являющиеся элементами конечного поля $GF(p^s)$, где p — простое число (характеристика поля) и $s \geq 1$ — степень расширения поля. Сложение векторов определяется по формуле

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

Одноразмерные векторы вида $k\mathbf{v}$, где $k \in GF(p^s)$ и $\mathbf{v}$ — некоторый формальный базисный вектор, входящие во вторую форму записи векторов, представляют собой компоненты вектора. Операция умножения векторов ($\circ$) определяется по естественному правилу попарного перемножения всех компонентов векторов-сомножителей по формуле

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

в которой вместо каждого из произведений двух базисных векторов подставляется однокомпонентный вектор, определяемый по специально задаваемой таблице умножения базисных векторов (ТУБВ). Координата этого однокомпонентного вектора называется коэффициентом растяжения. Совокупность клеток ТУБВ, в которых присутствует один и тот же коэффициент растяжения, определяет тип распределения этого коэффициента. В случае, когда определенная с помощью ТУБВ операция умножения векторов является ассоциативной, конечное векторное пространство является векторным конечным кольцом (ВКК). При этом мультипликативная группа кольца генерируется некоторым набором из r векторов $Z_1, Z_2, ..., Z_r$, называемым системой образующих. Система образующих, включающая минимально возможное число элементов группы, называется минимальной. Любой вектор из этой группы представим в виде произведения некоторых степеней элементов $Z_1, Z_2, ..., Z_r$. Частный вид такого строения, относящийся к случаю равенства порядков всех элементов минимальной системы образующих, называется строением с r-мерной цикличностью [3]. Конкретное значение r 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.

■ *Общий тип распределения растягивающих коэффициентов* ε *и* μ

$\circ$	**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**	$\varepsilon\mu$**e**
j	**j**	ε**k**	ε**u**	ε**v**	ε...	ε...	ε**z**	$\varepsilon\mu$**e**	μ**i**
k	**k**	ε**u**	ε**v**	ε...	ε...	ε**z**	$\varepsilon\mu$**e**	μ**i**	μ**j**
u	**u**	ε**v**	ε...	ε...	ε**z**	$\varepsilon\mu$**e**	μ**i**	μ**j**	μ**k**
v	**v**	ε...	ε...	ε**z**	$\varepsilon\mu$**e**	μ**i**	μ**j**	μ**k**	μ**u**
...	...	ε...	ε**z**	$\varepsilon\mu$**e**	μ**i**	μ**j**	μ**k**	μ**u**	μ**v**
...	...	ε**z**	$\varepsilon\mu$**e**	μ**i**	μ**j**	μ**k**	μ**u**	μ**v**	μ...
z	**z**	$\varepsilon\mu$**e**	μ**i**	μ**j**	μ**k**	μ**u**	μ**v**	μ...	μ...

Векторные конечные поля формируются при следующих условиях [4]:

1) размерность векторного пространства является делителем числа $p^s - 1$, т. е. $m \mid p^s - 1$;

2) в ТУБВ присутствуют коэффициенты растяжения, которые не могут быть представлены в виде d-й степени какого-либо элемента базового поля $GF(p^s)$, где $s \geq 2$, $d > 1$ — нетривиальный делитель размерности m.

При задании векторов в качестве поля $GF(p)$ используется кольцо $\boldsymbol{Z}_p$, а в качестве поля $GF(p^s)$, где $s \geq 2$, — конечные поля многочленов. Существует два общих типа распределения коэффициентов растяжения (таблица), обеспечивающих формирование ВКП [5] для произвольных значений m. Для заданного значения m имеется большое число других вариантов ТУБВ, которые зависят от конкретного значения m. Для любых ТУБВ, задающих коммутативное и ассоциативное умножение векторов, имеет место формирование конечных групп векторов с многомерной цикличностью, включая одномерную цикличность как частный случай.

Гомоморфизм конечных групп двухмерных и трехмерных векторов

При $m = 2$ общие правила умножения базисных векторов, обеспечивающие свойства коммутативности и ассоциативности операции умножения векторов, описываются следующими соотношениями: $\mathbf{e} \circ \mathbf{e} = \mathbf{e}$; $\mathbf{e} \circ \mathbf{i} = \mathbf{i} \circ \mathbf{e} = \mathbf{i}$ и $\mathbf{i} \circ \mathbf{i} = \varepsilon\mathbf{e}$, в соответствии с которыми можно записать формулу для умножения векторов $Z = (a\mathbf{e} + b\mathbf{i})$ и $Z' = (a'\mathbf{e} + b'\mathbf{i})$:

$$Z'' = Z \circ Z' = (a\mathbf{e} + b\mathbf{i}) \circ (a'\mathbf{e} + b'\mathbf{i}) = \\ = (aa' + \varepsilon bb')\mathbf{e} + (ab' + ba')\mathbf{i}. \qquad (1)$$

В двухмерном случае другие варианты задания ассоциативного умножения векторов не установлены. Нейтральным элементом по умножению является вектор $E = (1, 0)$. Множество всех векторов $\{Z\}$ такое, что каждому вектору Z может быть сопоставлен обратный вектор Z^{-1}, для которого выполняется соотношение $Z \circ Z^{-1} = E$, образует конечную группу. Рассмотрим решение уравнений вида $Z \circ X = E$, которое можно представить следующим образом:

$$(a\mathbf{e} + b\mathbf{i}) \circ (x\mathbf{e} + y\mathbf{i}) = 1\mathbf{e} + 0\mathbf{i}.$$

Для определения обратного значения Z^{-1} следует решать систему из двух линейных уравнений с двумя неизвестными x и y

$$\begin{cases} ax + \varepsilon by = 1 \\ bx + ay = 0 \end{cases}. \qquad (2)$$

Рассмотрим множество всех двухмерных векторов, заданных над конечным полем F, с определенной выше операцией умножения. Имеет место следующий гомоморфизм.

Утверждение 1. Главный определитель системы (2) задает гомоморфное отображение множества двухмерных векторов над конечным полем в конечное поле, над которым заданы векторы.

Доказательство: Пусть $Z = (a, b)$, $Z' = (a', b')$ и $Z'' = (a'', b'')$. Запишем главные определители системы (2) для векторов Z, Z' и Z'', причем координаты вектора Z'' сразу выразим через координаты векторов Z и Z' по формуле (1):

$$\Delta(Z) = \begin{vmatrix} a & \varepsilon b \\ b & a \end{vmatrix}; \quad \Delta(Z') = \begin{vmatrix} a' & \varepsilon b' \\ b' & a' \end{vmatrix}$$

$$\text{и } \Delta(Z'') = \begin{vmatrix} aa' + \varepsilon bb' & \varepsilon(ab' + ba') \\ ba' + ab' & \varepsilon bb' + aa' \end{vmatrix}.$$

Непосредственная проверка показывает, что $\Delta(Z) \cdot \Delta(Z') = \Delta(Z'')$, т. е. образ произведения равен произведению образов. Последнее означает, что отображение $\varphi(Z) = \Delta(Z)$, ставящее в соответствие каждому двухмерному вектору Z некоторый элемент базового поля, является гомоморфизмом. Утверждение доказано.

В синтезе алгоритмов ЭЦП на основе ВКК используются мультипликативные группы векторов. Очевидно, что доказанный гомоморфизм ВКК в базовое поле задает также и гомоморфизм мультипликативной группы векторов в мультипликативную группу базового поля. Отличие только в том, что гомоморфизм ВКК в базовое поле дополнительно включает отображение необратимых векторов в нулевой элемент базового поля. Это замечание имеет силу также и для случаев других размерностей векторного пространства, рассматриваемых ниже.

При $m = 3$ общие правила умножения базисных векторов, обеспечивающие свойства коммутативности и ассоциативности операции умножения векторов, описываются соотношениями $\mathbf{e} \circ \mathbf{e} = \mathbf{e}$; $\mathbf{e} \circ \mathbf{i} = \mathbf{i} \circ \mathbf{e} = \mathbf{i}$; $\mathbf{e} \circ \mathbf{j} = \mathbf{j} \circ \mathbf{e} = \mathbf{j}$; $\mathbf{i} \circ \mathbf{i} = \varepsilon\mathbf{j}$; $\mathbf{i} \circ \mathbf{j} = \mathbf{j} \circ \mathbf{i} = \varepsilon\mu\mathbf{e}$ и $\mathbf{j} \circ \mathbf{j} = \mu\mathbf{i}$, из которых вытекает следующая формула для умножения векторов $Z = (a\mathbf{e} + b\mathbf{i} + c\mathbf{j})$ и $Z' = (a'\mathbf{e} + b'\mathbf{i} + c'\mathbf{j})$:

$$\begin{aligned} Z'' = Z \circ Z' = (a\mathbf{e} + b\mathbf{i} + c\mathbf{j}) \circ (a'\mathbf{e} + b'\mathbf{i} + c'\mathbf{j}) = \\ = (aa' + \varepsilon\mu bc' + \varepsilon\mu cb')\mathbf{e} + (ab' + ba' + \mu cc')\mathbf{i} + \\ + (ac' + \varepsilon bb' + ca')\mathbf{j}. \end{aligned} \qquad (3)$$

Легко проверить, что нейтральным элементом по умножению является вектор $E = (1, 0, 0)$. Обращение вектора Z связано с решением векторного уравнения

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j}) = 1\mathbf{e} + 0\mathbf{i} + 0\mathbf{j},$$

откуда получаем систему из трех линейных уравнений с тремя неизвестными x, y и z вида

$$\begin{cases} ax + \varepsilon\mu cy + \varepsilon\mu bz \equiv 1 \\ bx + ay + \mu cz \equiv 0 \\ cx + \varepsilon by + az \equiv 0 \end{cases}. \qquad (4)$$

Рассмотрим множество всех трехмерных векторов, заданных над конечным полем F, с операцией умножения. Имеет место следующий гомоморфизм.

Утверждение 2. Главный определитель системы (4) задает гомоморфное отображение множества трехмерных векторов над конечным полем в конечное поле, над которым заданы векторы.

Доказательство: Пусть $Z = (a, b, c)$, $Z' = (a', b', c')$ и $Z'' = (a'', b'', c'')$. Запишем главные определители системы (4) для векторов Z, Z' и Z'':

$$\Delta(Z) = \begin{vmatrix} a & \varepsilon\mu c & \varepsilon\mu b \\ b & a & \mu c \\ c & \varepsilon b & a \end{vmatrix};$$

$$\Delta(Z') = \begin{vmatrix} a' & \varepsilon\mu c' & \varepsilon\mu b' \\ b' & a' & \mu c' \\ c' & \varepsilon b' & a' \end{vmatrix}$$

$$\text{и } \Delta(Z'') = \begin{vmatrix} a'' & \varepsilon\mu c'' & \varepsilon\mu b'' \\ b'' & a'' & \mu c'' \\ c'' & \varepsilon b'' & a'' \end{vmatrix}.$$

Значения этих определителей являются элементами базового поля, над которым заданы векторы. Перемножение первых двух определителей дает следующий определитель:

$$\Delta(Z)\cdot\Delta(Z') = \begin{vmatrix} aa'+\varepsilon\mu cb'+\varepsilon\mu bc' & \varepsilon\mu(ac'+ca'+\varepsilon bb') & \varepsilon\mu(ab'+\mu cc'+ba') \\ ba'+ab'+\mu cc' & \varepsilon\mu bc'+aa'+\varepsilon\mu cb' & \mu(\varepsilon bb'+ac'+ca') \\ ca'+\varepsilon bb'+ac' & \varepsilon(\mu cc'+ba'+ab') & \varepsilon\mu cb'+\varepsilon\mu bc'+aa' \end{vmatrix}. \quad (5)$$

Из (3) и (5) непосредственно следует $\Delta(Z)\cdot\Delta(Z') = \Delta(Z'')$, т. е. отображение $\varphi(Z) = \Delta(Z)$, ставящее в соответствие каждому трехмерному вектору Z элемент базового поля, является гомоморфизмом. Утверждение доказано.

Гомоморфизм в четырехмерном случае

Используя ТУБВ, записанную для четырехмерного случая, легко получить формулу, непосредственно описывающую результат $Z'' = Z \circ Z'$ умножения векторов $Z = (a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})$ и $Z' = (a'\mathbf{e} + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k})$:

$$\begin{gathered} Z'' = (a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \circ (a'\mathbf{e} + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = \\ = (aa' + \varepsilon\mu db' + \varepsilon\mu cc' + \varepsilon\mu bd')\mathbf{e} + (ba' + ab' + \mu dc' + \mu cd')\mathbf{i} + \\ + (ca' + \varepsilon bb' + ac' + \mu dd')\mathbf{j} + (da' + \varepsilon cb' + \varepsilon bc' + ad')\mathbf{k}. \end{gathered} \quad (6)$$

Единичным вектором является $E = (1, 0, 0, 0)$. Обращение вектора Z связано с решением векторного уравнения

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}) = 1\mathbf{e} + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k},$$

откуда вытекает система из четырех линейных уравнений с неизвестными x, y, z и w:

$$\begin{cases} ax + \varepsilon\mu dy + \varepsilon\mu cz + \varepsilon\mu dw = 1 \\ bx + ay + \mu dz + \mu cw = 0 \\ cx + \varepsilon by + az + \mu dw = 0 \\ dx + \varepsilon cy + \varepsilon bz + aw = 0 \end{cases}. \quad (7)$$

Рассмотрим множество всех четырехмерных векторов, заданных над конечным полем F, с операцией умножения. Имеет место следующий гомоморфизм.

Утверждение 3. Главный определитель системы линейных уравнений (7) задает гомоморфное отображение множества четырехмерных векторов над конечным полем в конечное поле, над которым заданы векторы.

Доказательство: Пусть $Z = (a, b, c, d)$, $Z' = (a', b', c', d')$ и $Z'' = (a'', b'', c'', d'')$. Запишем главные определители системы (7) для векторов Z, Z' и Z'':

$$\Delta(Z) = \begin{vmatrix} a & \varepsilon\mu d & \varepsilon\mu c & \varepsilon\mu b \\ b & a & \mu d & \mu c \\ c & \varepsilon b & a & \mu d \\ d & \varepsilon c & \varepsilon b & a \end{vmatrix}; \ \Delta(Z') = \begin{vmatrix} a' & \varepsilon\mu d' & \varepsilon\mu c' & \varepsilon\mu b' \\ b' & a' & \mu d' & \mu c' \\ c' & \varepsilon b' & a' & \mu d' \\ d' & \varepsilon c' & \varepsilon b' & a' \end{vmatrix} \text{ и } \Delta(Z'') = \begin{vmatrix} a'' & \varepsilon\mu d'' & \varepsilon\mu c'' & \varepsilon\mu b'' \\ b'' & a'' & \mu d'' & \mu c'' \\ c'' & \varepsilon b'' & a'' & \mu d'' \\ d'' & \varepsilon c'' & \varepsilon b'' & a'' \end{vmatrix}.$$

Перемножение определителей $\Delta(Z)$ и $\Delta(Z')$ дает следующий определитель:

$$\begin{vmatrix} aa'+\varepsilon\mu db'+\varepsilon\mu cc'+\varepsilon\mu bd' & \varepsilon\mu(ad'+da'+\varepsilon cb'+\varepsilon bc') & \varepsilon\mu(ac'+\mu dd'+ca'+\varepsilon bb') & \varepsilon\mu(ab'+\mu dc'+\mu cd'+ba') \\ ba'+ab'+\mu dc'+\mu cd' & \varepsilon\mu bd'+aa'+\varepsilon\mu db'+\varepsilon\mu cc' & \mu(\varepsilon bc'+ad'+da'+\varepsilon cb') & \mu(\varepsilon bb'+ac'+\mu dd'+ca') \\ ca'+\varepsilon bb'+ac'+\mu dd' & \varepsilon(\mu cd'+ba'+ab'+\mu dc') & \varepsilon\mu cc'+\varepsilon\mu bd'+aa'+\varepsilon\mu db' & \mu(\varepsilon cb'+\varepsilon bc'+ad'+da') \\ da'+\varepsilon cb'+\varepsilon bc'+ad' & \varepsilon(\mu dd'+ca'+\varepsilon bb'+ac') & \varepsilon(\mu dc'+\mu cd'+ba'+ab') & \varepsilon\mu db'+\varepsilon\mu cc'+\varepsilon\mu bd'+aa' \end{vmatrix}. \quad (8)$$

Из сравнения (6) и (8) непосредственно следует $\Delta(Z)\cdot\Delta(Z') = \Delta(Z'')$, т. е. отображение $\varphi(Z) = \Delta(Z)$, ставящее в соответствие каждому четырехмерному вектору Z элемент базового поля, является гомоморфизмом. Утверждение доказано.

Гомоморфизм конечных групп многомерных векторов

Предложения, аналогичные утверждениям 1, 2 и 3, можно доказать для значений размерности векторов $m \geq 5$. Авторы выполнили такое доказательство для $m = 5$, $m = 6$ и $m = 7$ в случае использования приведенной выше ТУБВ для определения операции умножения. Однако при достаточно больших m доказательство становится весьма громоздким. С целью проверить гипотезу о существовании указанного изоморфизма для произвольных значений размерности была разработана программа для ЭВМ, реализующая вычисление определителя, задающего гомоморфизм, и умножение векторов, определенное с помощью рассматриваемой ТУБВ. Вычислительный эксперимент подтвердил существование такого гомоморфизма для значений $m = 2, 3, ..., 55$. Таким образом, рассматриваемый гомоморфизм представляется справедливым для произвольных значений размерности векторов. Формальное доказательство существования такого гомоморфизма в общем случае является актуальным, однако это составляет предмет самостоятельной математической задачи. Наличие данного гомоморфизма следует учитывать при разработке схем и алгоритмов ЭЦП на основе конечных групп векторов для того, чтобы устранить потенциальные атаки с его использованием.

Гомоморфизм и синтез схем ЭЦП на основе конечных групп векторов

Разработка алгоритмов ЭЦП, основанных на сложности дискретного логарифмирования в конечных группах, связана с использованием секретного ключа, представляющего собой некоторое число $x < q$, где q — достаточно большое простое число, являющееся порядком группы, и открытого ключа Y, вычисляемого путем возведения некоторого генератора группы G в степень x, т. е. по формуле $Y = G^x$. Применение такого способа генерации открытого ключа в случае синтеза схем ЭЦП на основе групп векторов будет допускать потенциальную атаку, связанную с использованием описанного выше гомоморфизма. Действительно, из условия $Y = G^x$ следует $y = g^{x'}$, где $y, g \in GF(p^s)$, $y = \Delta(Y)$ и $g = \Delta(G)$, т. е. задачу дискретного логарифмирования (ЗДЛ) в группе векторов можно связать с ЗДЛ в конечном поле $GF(p^s)$, над которым заданы векторы. Решая последнюю задачу, можно определить значение $x' \equiv x \bmod q'$, где q' — порядок элемента g в базовом поле $GF(p^s)$. В общем случае получим значение $x' \leq x$, однако определенная часть секретного ключа будет вычислена. Стойкая схема ЭЦП не должна допускать такой возможности. Устранение таких атак может быть достигнуто путем выбора вектора G такого, что $\Delta(G) = 1$, как это было предложено в работе [6] в случае разработки схем ЭЦП на основе конечных групп невырожденных матриц. Действительно, тогда гомоморфизм дает уравнение $1 = 1^{x'}$, которое выполняется при любом значении неизвестной x', т. е. из него нельзя получить какую-либо информацию о секретном ключе x.

Таким образом, в синтезе алгоритмов ЭЦП на основе групп векторов возникает вопрос о существовании векторов G порядка q таких, что $\Delta(G) = 1$. Ответ на этот вопрос в случае, когда для простого значения q выполняется условие $q > p^s - 1$, дает следующее утверждение, где рассматривается мультипликативная группа векторов, в которой умножение задано с использованием приведенной таблицы.

Утверждение 4. Пусть для некоторого вектора G, принадлежащего группе векторов над полем $GF(p^s)$, для которой имеет место установленный выше гомоморфизм, выполняется условие $q > p^s - 1$, где q — простой порядок вектора G. Тогда имеет место соотношение $\Delta(G) = 1$.

Доказательство: По условию, q — порядок вектора G, т. е. выполняется соотношение $G^q = E$, следовательно, в силу установленного гомоморфизма выполняется и соотношение $\Delta^q(G) = \Delta(E) = 1$. Последнее возможно только в двух случаях: либо $\Delta(G) = 1$, либо q — порядок некоторого отличного от нуля и единицы элемента поля $GF(p^s)$. Допустим, что имеет место второй случай, но тогда $q | p^s - 1$, поскольку порядок элемента поля делит порядок мультипликативной группы поля. Это противоречит условию утверждения $q > p^s - 1$. Таким образом, всегда имеет место первый случай. Утверждение доказано.

Утверждение 4 используется при построении схемы ЭЦП, основанной на векторных группах, заданных над простым полем $GF(p)$ и обладающих многомерной цикличностью своего строения.

Алгоритм ЭЦП на основе конечных групп векторов с многомерной цикличностью

Рассмотрим случай задания ВКК над простым полем $GF(p)$ с характеристикой, удовлетворяющей условию $m | p-1$. Мультипликативная группа таких ВКК имеет r-мерное циклическое строение, где $r | m$ [3]. Ее минимальная система образующих включает r векторов, имеющих одинаковое значение порядка, а любой обратимый вектор Y может быть представлен как произведение некоторых степеней элементов, входящих в рассматриваемую систему образующих. Пусть q — мак-

симальный простой делитель порядка группы, тогда она содержит подгруппу порядка q^r, обладающую r-мерным циклическим строением и содержащую кроме единичного вектора только векторы порядка q. Минимальная система порождающих этой подгруппы содержит r векторов порядка q, которые обозначим как $G_1, G_2, ..., G_r$. Открытый ключ предлагается генерировать в виде r векторов $Y_1, Y_2, ..., Y_r$ по формуле

$$Y_i = G_1^{x_{i1}} \circ G_2^{x_{i2}} \circ \ldots \circ G_r^{x_{ir}}, \qquad (9)$$

где $i = 1, 2, ..., r$; $x_{i1}, x_{i2}, ..., x_{ir}$ — набор чисел, выбираемых по случайному закону и составляющих секретный ключ. Ниже описаны процедуры формирования и проверки подлинности подписи в схеме ЭЦП, построенной с использованием открытого ключа со структурой (9). Заметим, что мы предполагаем, что значение r лежит в пределах $1 < r < m$, т. е. $m = \delta r$ при некоторых целых $\delta < m$ и $r < m$. В этом случае при коэффициентах растяжения $\mu = 1$ и ε таком, что уравнение $x^\gamma = \varepsilon$ относительно неизвестной x не имеет решений в поле $GF(p)$ для всех отличных от единицы делителей $\gamma|\delta$, порядок мультипликативной группы ВКК выражается формулой

$$\Omega = (p^\delta - 1)^r,$$

причем максимальное значение порядка векторов

$$\omega_{\max} = p^\delta - 1 = (p-1)(p^{\delta-1} + p^{\delta-2} + \ldots + p + 1).$$

Для простого δ легко подобрать такие значения p, для которых число $q = \delta^{-1}(p^{\delta-1} + p^{\delta-2} + ... + p + 1)$ является простым и $\omega_{\max} = \delta(p-1)q$, где разрядность простого множителя q примерно в $\delta - 1$ раз превышает разрядность простого числа p, т. е. имеет место $q >> p - 1$ и для векторов G_i порядка q имеет место $\Delta(G_i) = 1$ (см. утверждение 4). Для синтеза алгоритмов ЭЦП представляет интерес использовать значения $\delta \in \{3, 5, 7, 11\}$ и $r \in \{2, 3, 4\}$, т. е. $6 \le m \le 44$. Рассмотрим вариант реализации схемы ЭЦП, заданной процедурами генерации и верификации ЭЦП.

Генерация подписи к сообщению M выполняется следующим образом.

1. Выбрать r случайных чисел $k_1, k_2, ..., k_r$ таких, что для всех $i = 1, 2, ..., r$ выполняется соотношение $k_i < q$.

2. Вычислить вектор $R = G_1^{k_1} \circ G_2^{k_2} \circ \ldots \circ G_r^{k_r}$.

3. Используя некоторую специфицированную хэш-функцию F_h (различные варианты хэш-функций представлены в работе [7]), вычислить значение хэш-функции h от сообщения M, к которому присоединен вектор R: $h = F_h(M, R)$, где длина $|h| \ge 160$ бит.

4. Представить h в виде конкатенации r значений $h_1, h_2, ..., h_r$, т. е. $h = h_1 \| h_2 \| ... \| h_r$, и вычислить второй элемент ЭЦП в виде набора r чисел $s_1, s_2, ..., s_r$:

$$s_i = k_i + \sum_{j=1}^{r} x_{ij} h_i \bmod q, \quad i = 1, 2, \ldots, r,$$

где условие $\sum_{i=1}^{r} |s_i| = r|q| \ge 160$ бит должно быть обеспечено выбором соответствующих параметров используемой группы векторов ($|s_i|$ обозначает длину двоичной записи числа s_i).

Проверка подлинности ЭЦП выполняется так.

1. Вычислить вектор

$$R^* = Y_1^{-h_1} \circ Y_2^{-h_2} \circ \ldots \circ Y_r^{-h_r} \circ G_1^{s_1} \circ G_2^{s_2} \circ \ldots \circ G_r^{s_r}.$$

2. Вычислить величину $h^* = F_h(M, R^*)$.

3. Сравнить значения h^* и h. Если $h^* = h$, то ЭЦП является подлинной.

Пример построения групп векторов для использования в рассмотренной выше схеме ЭЦП. Зададим значения $m = 6$ и $p = 3112656501667$ (векторы определяются над простым конечным полем). Определим операцию умножения шестимерных векторов $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} + h\mathbf{u} + l\mathbf{v}$ с помощью рассматриваемой ТУББВ при коэффициентах растяжения $\varepsilon = 4$ и $\mu = 1$. Значение 4 является квадратичным вычетом и кубичным невычетом по модулю 3112656501667, что задает формирование векторной группы с двухмерной цикличностью и $\Omega = (p^3 - 1)^r$, где $r = 2$. Максимальный простой делитель порядка группы равен $q = 3229543499124319810093519$. Данная группа шестимерных векторов содержит подгруппу Γ' порядка $\Omega' = q^2$, которая включает большое число подгрупп простого порядка, 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 = (2163836008099, 1269457016022, 1433319355034, 23538694425121, 674881435043, 911951500111)

и

G_2 = (2922266211036, 1381741886391, 1635981994737, 2434985478441, 1797895338418, 23924296834).

Проверка показала, что, действительно, в соответствии с утверждением 4 выполняются условия $\Delta(G_1) = 1$ и $\Delta(G_2) = 1$.

Заключение

Установленное гомоморфное отображение конечных групп векторов, заданных над конечным полем, в это поле доказано формально для значений размерности $m = 2$, 3 и 4. Аналогичным способом этот гомоморфизм доказывается для других сравнительно малых значений m. Для больших значений размерности справедливость установлена экспериментально путем выполнения соответствующих вычислительных экспериментов. Наличие такого гомоморфизма требуется учитывать при синтезе схем ЭЦП на основе конечных групп векторов. Предложен алгоритм ЭЦП на основе конечных групп векторов, строение которых обладает многомерной цикличностью. Реализация алгоритмов ЭЦП по данной схеме даст достаточно высокую производительность (в 5–30 раз более высокую по сравнению с известными алгоритмами ЭЦП). Однако данный тип конечных групп является новым криптографическим примитивом, и сложная задача нахождения дискретных логарифмов по многомерному основанию, положенная в основу предлагаемой схемы ЭЦП, требует детального самостоятельного изучения исследователями, специализирующимися в различных областях математики, криптографии и теории сложности. Такие исследования дадут в будущем этой схеме более полную и всестороннюю оценку, которая подтвердит ожидания авторов или потребует увеличения размеров параметров базовой конечной группы векторов для построения алгоритмов ЭЦП по предложенной схеме.

Для задания коммутативного и ассоциативного умножения векторов в конечном векторном пространстве могут быть использованы и другие варианты ТУБВ. Можно предположить, что установленный гомоморфизм будет иметь место для всех таких ТУБВ. Выполненные авторами частные проверки этой гипотезы подтвердили ее, но общее формальное доказательство наличия такого гомоморфизма для всех типов коммутативных и ассоциативных ТУБВ остается нерешенной проблемой, требующей самостоятельного исследования.

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

Литература

1. **Доронин С. Е., Молдовян Н. А., Синев В. С.** Конечные расширенные поля для алгоритмов электронной цифровой подписи // Информационно-управляющие системы. 2009. № 1. С. 33–40.
2. **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.
3. **Молдовян Н. А.** Многомерная цикличность групп векторов и их использование в алгоритмах аутентификации информации // Вестник СПбГУ. Сер. 10. 2009. В печати.
4. **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.
5. **Молдовян Д. Н., Молдовяну П. А.** Задание умножения в полях векторов большой размерности // Вопросы защиты информации. 2008. № 3(82). С. 12–17.
6. **Дернова Е. С., Костина А. А., Молдовяну П. А.** Конечные группы матриц как примитив алгоритмов цифровой подписи // Вопросы защиты информации. 2008. № 3(82). С. 8–12.
7. **Menezes A. J., Van Oorschot P. C., Vanstone S. A.** Handbook of Applied Cryptography. — Boca Raton, FL: CRC Press, 1997. — 780 p.