УДК 681.3

КОНЕЧНЫЕ РАСШИРЕННЫЕ ПОЛЯ ДЛЯ АЛГОРИТМОВ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Н. А. Молдовян,
доктор техн. наук, профессор, гл. научный сотрудник
НФ ФГУП НИИ «Вектор» — специализированный центр программных систем «Спектр»
С. Е. Доронин,
аспирант
В. Е. Синев,
аспирант
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

Описываются новые частные варианты реализации конечных расширенных полей, предназначенных для построения производительных алгоритмов электронной цифровой подписи. Показано, что новая форма представления конечных расширенных полей путем задания специальной операции умножения в конечном m-мерном векторном пространстве обеспечивает возможность эффективного распараллеливания вычислений, благодаря чему обеспечивается повышение производительности алгоритмов электронной цифровой подписи, основанных на конечных группах матриц и эллиптических кривых при их задании над конечными расширенными полями, представленными в новой форме.

Ключевые слова *— эллиптические кривые, цифровая подпись, векторные конечные поля, конечные группы матриц.*

Введение

Из известных алгебраических структур, применяемых для построения алгоритмов электронной цифровой подписи (ЭЦП), наибольшую производительность процедур формирования и проверки подлинности ЭЦП при заданном уровне стойкости обеспечивают конечные группы точек эллиптической кривой (ЭК) благодаря тому, что в качестве координат ЭК достаточно использовать элементы конечного поля, порядок которого имеет сравнительно малый размер (160–256 бит). Групповой операцией на ЭК является композиция (сложение) точек, для выполнения которой осуществляется одна операция инверсии и несколько операций умножения координат [1–3]. Операция инверсии вносит основной вклад в ограничение производительности алгоритмов аутентификации информации, построенных с использованием ЭК. Актуальной для практики задачей является дальнейшее повышение производительности алгоритмов ЭЦП. В случае использования ЭК уменьшение сложности операции композиции точек достигается при представлении ЭК в проективных координатах [3], когда устраняется операция инверсии в конечном поле, над которым задана ЭК, однако увеличивается число умножений в этом поле. Предложение использовать конечные группы невырожденных матриц (КГНМ), заданные над конечным полем, для построения алгоритмов ЭЦП [4] дает возможность дальнейшего повышения производительности алгоритмов ЭЦП, однако при этом в два раза увеличивается размер открытого ключа.

В случае использования ЭК и КГНМ для построения алгоритмов ЭЦП определяющим фактором, влияющим на производительности, является сложность операции умножения в конечном поле, над которым задаются эти алгебраические структуры, и невозможность распараллеливания этой операции при использовании известных форм задания конечных полей. В известных реализациях ЭК и КГНМ используется простое поле, представленное кольцом Z_p, где p — простое число, или расширенное конечное поле многочленов. В первом случае умножение элементов поля реализуется как умножение чисел по модулю p, а во втором случае — как умножение многочленов по модулю неприводимого многочлена. Оба типа операции модульного умножения реализуются

с использованием операции обычного умножения и деления результата на простое число или неприводимый многочлен соответственно. Это не позволяет распараллелить операцию умножения в конечном поле с целью повысить производительности алгоритмов ЭЦП.

В настоящей работе для задания ЭК и КГНМ предлагается использовать конечные расширенные поля, формируемые в конечных m-мерных векторных пространствах, в которых операция умножения является распараллеливаемой по определению, а именно, координаты вектора-результата вычисляются независимо друг от друга. Это позволяет при аппаратной реализации существенно повысить производительность алгоритмов ЭЦП, использующих вычисления на ЭК или в КГНМ. Общая схема синтеза алгоритмов ЭЦП на основе ЭК и КГНМ остается прежней. Изменяется только форма представления конечного поля, над которым задаются эти структуры. Ввиду известного факта о изоморфизме всех конечных полей заданного порядка ожидается, что такая замена формы представления конечного поля не приведет к изменению структурных свойств ЭК и КГНМ и сложности задачи дискретного логарифмирования на ЭК или в КГНМ, которая определяет безопасность алгоритмов ЭЦП, построенных с использованием ЭК и КГНМ. В связи с этим в статье акцент делается на способ задания конечных расширенных полей в новой форме и условиях их формирования.

Конечные расширенные поля векторов над полем $GF(p)$

Рассмотрим конечное множество m-мерных векторов

$$a\mathbf{e} + b\mathbf{i} + ... + c\mathbf{j},$$

где **e**, **i**, ... **j** — базисные векторы, которые будем представлять также и в виде набора координат $(a, b, ..., c)$, являющихся элементами конечного поля $GF(p)$, где p — простое число. В дальнейшем нас будут интересовать условия, при которых рассматриваемое множество векторов будет обладать свойствами расширенного поля, поэтому определим на этом множестве две операции — сложение и умножение векторов. Операцию сложения векторов определим по следующему естественному правилу:

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

Операцию умножения векторов определим по правилу умножения многочленов с учетом того, что умножение базисных векторов выполняется по некоторым табличным правилам, ставящим в соответствие каждой паре умножаемых базисных векторов третий базисный вектор (возможно, совпадающий с одним из перемножаемых базисных векторов) или третий базисный вектор, умноженный на некоторый коэффициент ε, являющийся элементом поля $GF(p)$. Таким образом, имеем

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

где каждое из произведений **ee**, **ei**, ..., **ej**, **ie**, **ii**, ..., **ij**, **je**, **ji**, ..., **jj** следует заменить на задаваемое таблицей умножения базисных векторов значение ε**v**, где **v** — вектор, принадлежащий множеству базисных векторов. Синтез таблицы является определяющим моментом в задании конкретного варианта операции умножения, которая определяет тип алгебраической структуры, формируемой в конечном пространстве m-мерных векторов при заданном поле $GF(p)$. Таблица умножения базисных векторов определяет над их множеством некоторую операцию. Нас интересует случай образования конечных групп в пространстве m-мерных векторов, поэтому указанная таблица должна быть составлена с учетом обеспечения свойства ассоциативности умножения базисных векторов. В общем случае порядок умножаемых базисных векторов имеет значение, однако мы ограничимся рассмотрением наиболее интересного для нас случая задания коммутативной операции умножения базисных векторов. Легко показать, что свойство коммутативности и ассоциативности умножения базисных векторов естественным способом переходит в свойство коммутативности и ассоциативности умножения m-мерных векторов. При выполнении этого условия в конечном векторном пространстве формируются структуры со свойствами коммутативной группы. Конкретные варианты таблиц, задающих правила умножения базисных векторов, рассмотрены далее.

Ниже будет показано, что при определенных соотношениях между размерностью векторов m и порядком поля p в частных случаях задания операции умножения векторов формируются конечные расширенные поля $GF(p^m)$. Сравним сложность операции умножения в поле такого типа со сложностью умножения в простом поле $\boldsymbol{Z}_{p'}$, где $|p'| = m|p|$ и $|p|$ обозначает битовую длину числа p (т. е. в случае полей с одинаковым размером порядка). Операция умножения элементов поля $GF(p^m)$ включает m^2 операций умножения в поле $GF(p)$, причем сложность операции умножения в поле $GF(p)$ пропорциональна $|p|^2$, поэто-

му при прямолинейном выполнении операции умножения в поле $GF(p^m)$, представленном в векторной форме, ее сложность примерно равна сложности умножения в поле Z_p, (операции арифметического сложения мы не учитываем, поскольку их вклад достаточно мал).

Однако имеется возможность снизить сложность умножения элементов поля $GF(p^m)$ следующим образом. Осуществляются обычные арифметические операции умножения соответствующих пар координат векторов-сомножителей, результаты суммируются, а затем выполняется операция арифметического деления полученного результата на значение p. При этом число арифметических умножений остается равным m^2, а число делений уменьшается в m раз, становясь равным m. При этом сложность операции деления возрастает за счет увеличения делимого несущественно, так как размер последнего увеличивается всего лишь в m раз, т. е. его длина возрастает на несколько битов. Это не вносит существенного увеличения сложности операции деления в случае практически значимых размеров значений координат, которые определяются размерами модуля от $|p| = 16$ до $|p| = 200$ бит для значений размерности от $m = 13$ до $m = 3$ соответственно. Поскольку сложность операции деления значительно превосходит сложность операции умножения, то сложность операции умножения элементов поля $GF(p^m)$ снижается примерно пропорционально значению m. Наличие дополнительных операций умножения на коэффициенты растяжения, используемые для создания условия формирования полей в конечных векторных пространствах, не вносит существенного вклада в общую сложность всех операций арифметического умножения, поскольку в качестве таких коэффициентов можно подобрать числа размером в 2–3 бит.

Рассмотрим сложность умножения в поле $GF(p^m)$, заданном в виде конечного кольца многочленов степени $m - 1$. Операция умножения двух многочленов включает m^2 операций арифметического умножения $|p|$-битовых чисел и m операций деления $2|p|$-битовых чисел на модуль p (операциями сложения пренебрегаем ввиду их низкой сложности). В результате получаем многочлен степени $2m - 2$, который далее делится на неприводимый многочлен. Наличие этой операции не допускает эффективного распараллеливания операции умножения в поле многочленов. Наиболее эффективная реализация деления на неприводимый многочлен требует выполнения примерно m^2 операций арифметического умножения $|p|$-битовых чисел и m операций деления $2|p|$-битовых чисел на модуль p. Видим, что в целом операция умножения в поле многочленов, по крайней мере, в два раза сложнее операции умножения в поле $GF(p^m)$, заданном в векторном пространстве.

Таким образом, переход к новой форме задания расширенных конечных полей дает выигрыш в вычислительной эффективности *даже в случае использования однопроцессорного вычислительного устройства*. При этом операция умножения в поле $GF(p^m)$, заданном в конечном векторном пространстве, обладает возможностью эффективного распараллеливания на m процессов, поэтому при увеличении сложности аппаратной реализации имеется возможность сократить время выполнения умножения в поле $GF(p^m)$ примерно до m^2 раз в сравнении с простым полем и до $2m$ раз в сравнении с конечным полем многочленов. (Процедуры, входящие в операцию умножения в поле многочленов и выполняемые до деления на неприводимый многочлен, могут быть выполнены параллельно, но это увеличивает аппаратные затраты, приводя к уменьшению времени выполнения умножения в поле многочленов всего лишь в $2m(m + 1)^{-1}$ раз. В сравнении с этим вариантом реализации операции умножения многочленов распараллеливание операции умножения в векторном поле дает сокращение времени в m раз.)

Конечные группы и поля в пространстве трехмерных векторов

При $m = 3$ общие правила умножения базисных векторов, обеспечивающие свойства коммутативности и ассоциативности операции умножения векторов, представлены в табл. 1, где ε и μ — коэффициенты растяжения, $\varepsilon, \mu \in GF(p)$. В зависимости от конкретной пары значений ε и μ множество трехмерных векторов является конечным полем или конечной группой. Поскольку определенные нами операции сложения и умножения векторов являются коммутативными и ассоциативными, а операция умножения дистрибутивна по отношению к операции сложения, то конечное пространство трехмерных векторов будет образовывать расширенное поле $GF(p^3)$, если для каждого отличного от (0, 0, 0) трехмерного вектора существует вектор, являющийся обратным к нему. В противном случае будем иметь группу, порядок которой определяется числом векторов, для которых существуют соответствующие обратные элементы. Решение этого вопроса связано с анализом характеристического уравнения третьей степени, возникающего из условия существования вектора $(x\mathbf{e} + y\mathbf{i} + z\mathbf{j})$, являющегося обратным значением к векторам вида $a\mathbf{e} + b\mathbf{i} + c\mathbf{j}$, где хотя бы одна из координат a, b, c отлична от нуля. Исходя из условия существования обрат-

ных значений запишем в соответствии с табл. 1 и общим определением операции умножения векторов следующее соотношение:

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j})(x\mathbf{e} + y\mathbf{i} + z\mathbf{j}) = (ax + \varepsilon\mu cy + \mu\varepsilon bz)\mathbf{e} + (bx + ay + \mu cz)\mathbf{i} + (az + \varepsilon by + az)\mathbf{j},$$

из которого видно, что вопрос существования обратных значений сводится к вопросу существования решений системы уравнений вида

$$\begin{cases} ax + \varepsilon\mu cy + \varepsilon\mu bz = 1 \\ bx + ay + \mu cz = 0 \\ cx + \varepsilon by + az = 0 \end{cases}.$$

Равенство нулю главного определителя этой системы для некоторых троек значений (a, b, c) задает векторы $a\mathbf{e} + b\mathbf{i} + c\mathbf{j}$, для которых не существует обратных элементов. Таким образом, получаем следующее характеристическое уравнение:

$$a^3 - 3\varepsilon\mu bca + \varepsilon^2\mu b^3 + \varepsilon\mu^2 c^3 \equiv 0 \bmod p.$$

Используя формулу Кардано [5] и обозначение $B = (\varepsilon^2\mu b^3 + \varepsilon\mu^2 c^3)/2$, решение последнего уравнения относительно неизвестного a можно записать в виде

$$a_0 = A' + A'',$$

где

$$A' = \sqrt[3]{B + \sqrt{B^2 - (\varepsilon\mu bc)^3}} = \sqrt[3]{-\varepsilon\mu^2 c^3} \pmod p \text{ и}$$

$$A'' = \sqrt[3]{B - \sqrt{B^2 - (\varepsilon\mu bc)^3}} = \sqrt[3]{-\varepsilon^2\mu b^3} \pmod p.$$

Из исследования характеристического уравнения вытекают следующие типовые варианты структур рассматриваемого множества трехмерных векторов.

Случай 1. Число 3 не делит $p - 1$. Существует единственное значение кубичного корня для всех значений подкоренного выражения. В этом случае число корней характеристического уравнения определяется значением его дискриминанта [5]

$$D = -27\left(\varepsilon^2\mu b^3 - \varepsilon\mu^2 c^3\right)^2 \pmod p.$$

Если $c \equiv b\sqrt[3]{\varepsilon} \bmod p$, то $D = 0$ и существует два разных корня a'_0 и a''_0, поэтому для $2(p - 1)$ векторов вида $\left(a'_0, b, b\sqrt[3]{\varepsilon} \bmod p\right)$ и $\left(a''_0, b, b\sqrt[3]{\varepsilon} \bmod p\right)$, где $b \in \{1, 2, ..., p - 1\}$, не существует обратных значений. Если $c \neq b\sqrt[3]{\varepsilon} \bmod p$, то $D \neq 0$ и существует только один корень a_0, поэтому для $p(p - 1)$ векторов вида (a_0, b, c), где $b, c \in \{1, 2, ..., p - 1\}$, не существует обратных значений. Учитывая также, что не существует обратного значения для вектора (0, 0, 0), и вычитая из полного числа трехмерных векторов число векторов, для которых не существует обратных значений, получаем формулу для порядка группы трехмерных векторов

$$\Omega = p^3 - 2(p - 1) - p(p - 1) - 1 = (p - 1)^2(p + 1).$$

Экспериментально установлено, что в рассматриваемом случае группа векторов является нециклической и содержит циклические подгруппы порядка, равного $\Omega' \le (p - 1)(p + 1)$. Случай таких групп при $p = Nk^2 + 1$ или $p = Nk^2 - 1$, где k — большое простое число и N – нечетное число, представляет значительный интерес для разработки алгоритмов ЭЦП, основанных на сложности вычисления корней большой простой степени, аналогичных алгоритмам, предложенным в работе [6].

Случай 2. Число 3 делит $p - 1$, и каждое из произведений $\varepsilon^2\mu$ и $\varepsilon\mu^2$ является кубичным вычетом в поле $GF(p)$. Анализ дискриминанта характеристического уравнения показывает, что для $h = 6(p - 1) - 3(p^2 + 9(p - 1) + 2$ векторов не существует обратных значений. Вычитая из полного числа векторов значение h, получаем порядок группы

$$\Omega = p^3 - h = (p - 1)^3.$$

Эксперимент показал, что в рассматриваемом случае группа векторов является нециклической и содержит циклические подгруппы порядка, равного $\Omega' \le (p - 1)$. Случай таких групп также представляет интерес для разработки алгоритмов ЭЦП (основанных на сложности вычисления корней большой простой степени).

Случай 3. Число 3 делит $p - 1$, и каждое из произведений $\varepsilon^2\mu$ и $\varepsilon\mu^2$ является кубичным невычетом в поле $GF(p)$. Это может иметь место, например, в случае, когда ε — кубичный вычет, а μ — кубичный невычет, или наоборот. Тогда существует единственная пара значений b и c, а именно

■ ***Таблица 1.*** *Таблица умножения базисных векторов трехмерного пространства*

×	**e**	**i**	**j**
e	**e**	**i**	**j**
i	**i**	ε**j**	$\varepsilon\mu$**e**
j	**j**	$\varepsilon\mu$**e**	μ**i**

$b = c = 0$, для которой имеется решение $a_0 = 0$ характеристического уравнения. Это означает, что в этом случае каждому ненулевому вектору можно сопоставить обратный вектор. Следовательно, в рассматриваемом случае совокупность всех трехмерных векторов образует поле $GF(p^3)$, мультипликативная группа которого является циклической и имеет порядок

$$\Omega = p^3 - 1 = (p - 1)(p^2 + p + 1).$$

Эксперимент показывает, что и в этом случае легко найти такое значение p, при котором значение $\Omega' = (p^2 + p + 1)/3$ является простым. Циклические подгруппы такого порядка представляют интерес для построения алгоритмов ЭЦП, основанных на сложности задачи дискретного логарифмирования в поле трехмерных векторов.

Случай 4. При $\varepsilon = 0$, либо $\mu = 0$, либо $\varepsilon = 0$ и $\mu = 0$ имеем «вырожденный случай», когда характеристическое уравнение имеет вид $a^3 \equiv 0 \bmod p$ и единственное решение $a_0 = 0$ для всех пар значений b и c. Для этого случая получаем следующее значение порядка группы:

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

Эксперимент показал, что такая группа векторов является нециклической и содержит циклические подгруппы порядка, равного $\Omega' \le p(p - 1)$.

Пример 1. *Векторное поле* $GF(p^3)$. Для простого $p = 604884627778815030120967$ и коэффициентов $\mu = 1$ и $\varepsilon = 3048145277787150301203$ (кубичный невычет) генератором мультипликативной группы поля $GF(p^3)$ является вектор $\mathbf{G}_\Omega = 2\mathbf{e} + 3\mathbf{i} + 5\mathbf{j}$, а генератором подгруппы простого порядка $q = 12196180430770520253333277444585228380992277120 19$ — вектор $\mathbf{G}_q = 2766732051010005739014 75\mathbf{e} + 3973984426601319676024 19\mathbf{i} + 5777541997290551329836 73\mathbf{j}$.

Поля многомерных векторов

Изучение вопроса существования полей векторов размерности $m \ge 4$ дало положительный ответ. Аналогично построению конечных полей трехмерных векторов, можно задать формирование полей многомерных векторов. Для того чтобы множество m-мерных векторов составляло поле $GF(p^m)$, следует выбирать поле $GF(p)$, для характеристики которого выполняется условие делимости $m \mid p - 1$. Кроме того, в соответствующую таблицу умножения базисных векторов надо ввести коэффициенты растяжения, значения которых являются невычетами степени m в поле $GF(p)$. В этом случае многомерные векторные пространства (для $m \ge 4$), над которыми заданы принятые выше операции сложения и умножения, могут составить конечное поле $GF(p^m)$. Рассмотрим некоторые частные варианты.

Случай $m = 4$. Определим операцию умножения четырехмерных векторов $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ с помощью табл. 2, которая обеспечивает свойство коммутативности и ассоциативности. Задавая различные конкретные значения растягивающих коэффициентов, можно задавать различные варианты полей $GF(p^4)$. Существует еще несколько вариантов таблиц, с помощью которых можно задать формирование векторного поля в конечном пространстве четырехмерных векторов, которые отличаются распределением базисных векторов и коэффициентов растяжения, а также числом последних и их значениями. Для генерации следующего частного примера использована табл. 2.

Пример 2. *Векторное поле* $GF(p^4)$. Для простого $p = 670657405878917$ и коэффициентов $\mu = 1$ и $\varepsilon = 33322555333777$ (невычет 4-й степени) генератором мультипликативной группы поля $GF(p^4)$ является вектор $\mathbf{G}_\Omega = 2\mathbf{e} + 5\mathbf{i} + 7\mathbf{j} + 11\mathbf{k}$, а генератором подгруппы максимального простого порядка $q = 51058526584281452221$ является вектор $\mathbf{G}_q = 387227204127143\mathbf{e} + 285726718179315\mathbf{i} + 399932449346308\mathbf{j} + 297703341165198\mathbf{k}$.

Случай $m = 5$. Определим операцию умножения пятимерных векторов $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} + g\mathbf{u}$ с помощью табл. 3, в которой присутствуют несколько различных независимых коэффициентов растяжения. При любой комбинации значений этих коэффициентов операция умножения

■ ***Таблица 2.*** *Таблица умножения базисных векторов для случая* $m = 4$

×	e	i	j	k
e	e	i	j	k
i	i	εμj	εk	εμe
j	j	εk	εe	i
k	k	εμe	i	μj

■ ***Таблица 3.*** *Таблица умножения базисных векторов для случая* $m = 5$

×	e	i	j	k	u
e	e	i	j	k	u
i	i	εj	εμk	εu	εμe
j	j	εμk	εμu	εμe	μi
k	k	εu	εμe	i	J
u	u	εμe	μi	j	μk

векторов является коммутативной и ассоциативной. При программной реализации операции умножения векторов в клетках таблицы, где присутствуют два или более растягивающих коэффициентов, значения последних следует перемножить, благодаря чему формируется таблица, в каждой клетке которой присутствует не более одного коэффициента. Табл. 3 использована для генерации следующего примера.

Пример 3. *Векторное поле* $GF(p^5)$. Для простого $p = 268675256028581$ и коэффициентов $\mu = 1$ и $\varepsilon = 3048145277787$ (невычет 5-й степени) генератором мультипликативной группы поля $GF(p^5)$ является вектор $\mathbf{G}_\Omega = 2\mathbf{e} + 5\mathbf{i} + 7\mathbf{j} + 11\mathbf{k} + 13\mathbf{u}$, а генератором подгруппы простого порядка $q = 10421\,75072703434265745203478134729214503105234181740193961$ — вектор $\mathbf{G}_q = 88815218764680\mathbf{e} + 238886012231841\mathbf{i} + 157317400153847\mathbf{j} + 21593513218048\mathbf{k} + 204824491909450\mathbf{u}$.

Формирование конечных полей для случая $m = 6$ можно обеспечить, используя табл. 4, а для случая $m = 7$ – табл. 5. Практическое значение для разработки алгоритмов ЭЦП, основанных на вычислениях в конечных группах ЭК и КГНМ, заданных над полями, представленными в предлагаемой форме, имеют также и случаи размерностей $m > 7$. Нами были построены таблицы умножения базисных векторов, обеспечивающие формирование полей, для произвольных значений размерности до $m = 23$. Для этих случаев эксперимент подтвердил существование полей при таких значениях размерности.

Найденные правила построения таблиц умножения базисных векторов, содержащих коэффициенты растяжения, позволяют обеспечить свойства коммутативности и ассоциативности умножения m-мерных векторов для произвольных значений размерности. Однако теоретическое доказательство факта возможности формирования полей по таким таблицам путем выбора соответствующих коэффициентов растяжения имеет принципиальные трудности и представляет самостоятельную задачу теории линейных алгебр. Объективная трудность такого доказательства определяется большой общностью этого факта. Для технических приложений представляется достаточным использование частных случаев значений размерности до $m = 23$, подтвержденных экспериментом. Если практика потребует использования конечных расширенных полей, заданных в векторном пространстве размерности $m > 23$, то экспериментальная проверка факта существования конечных полей и для таких случаев не составит существенных проблем.

■ ***Таблица 4.*** *Таблица умножения базисных векторов для случая* $m = 6$

×	**e**	**i**	**j**	**k**	**v**	**w**
e	**e**	**i**	**j**	**k**	**u**	**v**
i	**i**	ε**j**	$\varepsilon\mu$**k**	**u**	ε**v**	$\varepsilon\mu$**e**
j	**j**	$\varepsilon\mu$**k**	μ**u**	**v**	$\varepsilon\mu$**e**	μ**i**
k	**k**	**u**	**v**	**e**	**i**	**j**
u	**u**	ε**v**	$\varepsilon\mu$**e**	**i**	$\varepsilon\mu$**j**	$\varepsilon\mu$**k**
v	**v**	$\varepsilon\mu$**e**	μ**i**	**j**	$\varepsilon\mu$**k**	μ**u**

■ ***Таблица 5.*** *Таблица умножения базисных векторов для случая* $m = 7$

×	**e**	**i**	**j**	**k**	**u**	**v**	**w**
e	**e**	**i**	**j**	**k**	**u**	**v**	**w**
i	**i**	$\varepsilon\mu$**k**	$\varepsilon\nu$**v**	$\mu\tau$**u**	$\varepsilon\nu$**w**	$\varepsilon\mu\tau$**e**	$\mu\tau$**j**
j	**j**	$\varepsilon\nu$**v**	ε**u**	$\varepsilon\mu\tau$**e**	ε**i**	ε**w**	ε**k**
k	**k**	$\mu\tau$**u**	$\varepsilon\mu\tau$**e**	$\mu\tau$**w**	$\mu\tau$**j**	τ**i**	$\mu\tau$**v**
u	**u**	$\varepsilon\nu$**w**	ε**i**	$\mu\tau$**j**	$\varepsilon\nu$**v**	ε**k**	$\varepsilon\mu\tau$**e**
v	**v**	$\varepsilon\mu\tau$**e**	ε**w**	τ**i**	ε**k**	τ**j**	τ**u**
w	**w**	$\mu\tau$**j**	ε**k**	$\mu\tau$**v**	$\varepsilon\mu\tau$**e**	τ**u**	τ**v**

Алгоритмы ЭЦП с использованием конечных расширенных полей, заданных в новой форме

Рассмотренные выше конечные поля, представленные в векторной форме и допускающие эффективное распараллеливание операции умножения, представляют технический интерес для повышения быстродействия алгоритмов ЭЦП, построенных на основе использования ЭК и КГНМ, путем задания ЭК и КГНМ над такими полями. В случае ЭК вопрос стойкости алгоритмов ЭЦП связан с выбором ЭК соответствующего типа, определяемого значением характеристики поля (т. е. значением p), и выбором конкретного варианта ЭК, порядок которой делится на простое число большого размера. Методика генерации таких кривых хорошо апробирована [1, 2]. В случае КГНМ вопрос безопасности алгоритмов ЭЦП является весьма актуальным, поскольку это направление сравнительно мало освещено в литературе и вопрос стойкости алгоритмов на их основе исследован недостаточно. Касательно использования КГНМ в качестве примитивов алгоритмов ЭЦП, в настоящей работе преследуется цель только показать принципиальную возможность повышения производительности алгоритмов и в случае использования КГНМ. Этот факт представит значительный практический интерес, если дальнейшие специализированные исследования приведут к подтверждению высокой

сложности задачи дискретного логарифмирования в КГНМ, заданных над конечными полями размера 160–200 бит.

Следует отметить, что определенный интерес представляет также непосредственное применение конечных расширенных полей, представленных в новой форме. Рассмотрим возможный вариант обобщенной схемы ЭЦП, основанной на сложности дискретного логарифмирования в конечных расширенных полях, предполагая в нем использование циклической группы векторов Г. Подписывающий формирует свой открытый ключ Y в виде вектора $\mathbf{Y} = \mathbf{G}^x$, где $\mathbf{G}$ — вектор, являющийся генератором группы Г, имеющей достаточно большой порядок q ($|q| \geq 160$ бит).

Формирование подписи к сообщению M выполняется следующим образом.

1. Выбрать случайное число $k < q$ и вычислить вектор $\mathbf{R} = \mathbf{G}^k$.

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

3. Вычислить второй элемент ЭЦП: $s = xh + k \bmod q$.

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

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

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

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

Конкретный вариант алгоритмической реализации этой общей схемы ЭЦП задается выбором конкретной группы Г, характеризующейся размерностью векторов, заданным типом операции умножения векторов и полем $GF(p)$, над которым задается конечное векторное пространство. Многочисленные другие известные варианты схем ЭЦП [6–8], построенные с использованием простых конечных полей, могут быть заданы также и над полями, формируемыми в конечном векторном пространстве.

В целях реализации вычислительно эффективных алгоритмов ЭЦП, непосредственно базирующихся на полях в предлагаемой форме, требуется получить циклическую подгруппу векторов большого простого порядка q, размер которого удовлетворяет условиям $|q| \geq 160$ бит и $|q| \approx (m-1)|p|$. Последнее условие возможно только для простых значений m. Действительно, порядок мультипликативной группы конечного расширенного поля $GF(p^m)$ равен

$$\Omega = p^m - 1 = (p-1)(p^{m-1} + p^{m-2} + \ldots + p + 1).$$

Легко показать, что если размерность m не является простым числом, то вторая скобка разлагается на нетривиальные множители для любого простого числа p. При условии $m \mid p-1$ (которое имеет место в случае формирования векторных полей) сумма $p^{m-1} + p^{m-2} + \ldots + p + 1$ делится на m, поэтому простым может быть только порядок циклической подгруппы мультипликативной группы поля $GF(p^m)$, равный $q = m^{-1}(p^{m-1} + p^{m-2} + \ldots + p + 1)$. Эксперимент показывает, что легко найти такие значения простого p, для которых такое значение q также является простым. В этом случае имеем циклическую подгруппу векторов, размер порядка которой равен

$$|\Omega'| = |q| = (m-1)|p| - |m| \approx (m-1)|p|.$$

Для построения алгоритмов ЭЦП требуется использовать подгруппы простого порядка размером $|\Omega'| \geq$ **160 бит. Для этой цели следует формировать** поля m-мерных векторов, заданных над простым полем с размером характеристики $|p|$, удовлетворяющим условию

$$|p| \geq \frac{160 - |m|}{m-1} \approx \frac{160}{m-1} \text{ [бит]}.$$

Таким образом, важное требование наличия в мультипликативной группе поля подгруппы простого порядка достаточно большого размера реализуется при сравнительно малом размере $|p|$. Практическое значение для разработки алгоритмов ЭЦП, основанных на сложности задачи дискретного логарифмирования в новых полях, имеют случаи $m \in \{3, 5, 7, 11, 13, 17, 19, 23\}$.

В общем случае при построении векторных полей для непосредственного применения в алгоритмах ЭЦП, основанных на сложности задачи дискретного логарифмирования, таблицы умножения базисных векторов следует задавать с учетом компромисса между следующими моментами.

- В получаемой алгебраической структуре должны содержаться группы большого простого порядка, размер которого близок к значению $(m-1)|p|$.
- Количество умножений в поле $GF(p)$, необходимых для выполнения операции умножения двух векторов, следует минимизировать.
- Размер коэффициентов растяжения и число ячеек таблицы умножения базисных векторов, где они присутствуют, следует минимизировать.
- В получаемой циклической группе векторов сложность задачи дискретного логарифмирования (нахождение x в уравнении вида $\mathbf{Y} = \mathbf{G}^x$, где $\mathbf{G}$ — генератор группы) должна быть достаточно высокой.

Основной проблемой непосредственного использования конечных полей, заданных в предлагаемой форме, является то, что сложность задачи дискретного логарифмирования в них является новой. Поэтому повышение производительности путем снижения размера порядка поля

ниже 1024 бит, т. е. ниже безопасного значения, признанного в случае конечных полей многочленов, является преждевременным. Тем не менее, существенный выигрыш в производительности достигается благодаря снижению сложности операции умножения элементов поля и возможности эффективного распараллеливания в случае использования многопроцессорного вычислителя или за счет увеличения схемотехнических затрат в случае аппаратной реализации. С учетом этого можно предположить, что для некоторых приложений непосредственное применение полей, заданных в предлагаемой форме, также представит определенный интерес, поскольку достаточно высокая производительность алгоритмов ЭЦП, основанных на непосредственном использовании полей, заданных в конечном векторном пространстве, обеспечивается также и при больших размерах порядка такого поля.

Заключение

При обеспечении условия делимости числа $p - 1$ на m имеется возможность разработать таблицу умножения базисных векторов, определяющую формирование конечного расширенного поля в пространстве векторов, в котором операция умножения допускает эффективное распараллеливание. Кроме того, при заданном значении размера порядка поля в случае полей, заданных в новой форме, снижается сложность операции умножения элементов поля. Данное представление полей может быть использовано при построении алгоритмов ЭЦП, основанных на использовании ЭК и КГНМ, путем задания этих алгебраических структур над конечными полями предложенного вида. Также представляет интерес и непосредственное применение полей такого типа при построении алгоритмов ЭЦП, однако в последнем случае в настоящее время следует рекомендовать значения размера порядка поля, равные 1024 бит и более. Вопрос снижения этого значения в целях дальнейшего повышения производительности требует выполнения исследования сложности задачи дискретного логарифмирования в предлагаемом варианте расширенных полей, что составляет задачу самостоятельного исследования.

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

Литература

1. **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.
2. **Болотов А. А., Гашков С. Б., Фролов А. Б.** Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006. 274 с.
3. **Koblitz N. A.** Course in Number Theory and Cryptography. Berlin: Springer-Verlag, 2003. 236 p.
4. **Гурьянов Д. Ю., Дернова Е. С., Молдовян Н. А.** Построение алгоритмов электронной цифровой подписи на основе групп матриц малой размерности // Информационная безопасность регионов России: Материалы V Санкт-Петербургской межрегион. конф. СПОИСУ. СПб., 2007. С. 79–80.
5. **Курош А. Г.** Курс высшей алгебры. М.: Наука, 1971. 431 с.
6. **Молдовян Н. А.** Вычисление корней по простому модулю как криптографический примитив // Вестник СПбГУ. Сер. 10. 2008. Вып. 1. С. 101–106.
7. **Молдовян Н. А.** Практикум по криптосистемам с открытым ключом. СПб.: БХВ-Петербург, 2007. 298 с.
8. **Menezes A. J., Van Oorschot P. C., Vanstone S. A.** Handbook of Applied Cryptography. CRC Press, Boca Raton, FL, 1997. 780 p.