Записки научных
семинаров ПОМИ
Том 387, 2011 г.

Н. Н. Васильев, М. А. Рыбалкин

ПЕРЕСТАНОВОЧНЫЕ ДВУЧЛЕНЫ И ГРУППЫ, ПОРОЖДЕННЫЕ ИМИ

1. Введение

В современном информационном обществе криптография является основным инструментом обеспечения конфиденциальности. Способы защиты информации и способы вскрытия такой защиты развиваются постоянно, и данное развитие вряд ли будет когда-то завершено в связи с постоянно увеличивающимися вычислительными возможностями современных компьютеров.

Одной из основных задач, решаемых в криптографии, является задача посылки сообщения по незащищенному каналу связи. Традиционный способ решения данной задачи состоит в использовании схемы шифрования с открытым ключом, идея которой заключается в использовании публичной функции для шифрования посылаемых сообщений, и секретной функции для расшифровки сообщений. Криптостойкость таких схем основана на предположении о большой вычислительной сложности задачи обращения функции шифрования без знания секрета, на основе которого данная функция была построена.

Перестановочными многочленами называются многочлены, функции которых являются биекциями над рассматриваемым кольцом. Перспектива использования перестановочных многочленов в криптографических схемах с отрытым ключом, как кандидатов на роль функций шифрования, является одним из главных стимулов развития теории таких многочленов. В настоящий момент в самом распространенном криптографическом протоколе RSA с открытым ключом в качестве шифрующих функций используются одночлены. Использование более сложных перестановочных многочленов может повысить криптостойкость такого протокола. В представляемой работе исследуется вопрос о свойствах перестановочных двучленов над ко-

Ключевые слова: онечные поля, перестановочные полиномы, перестановочные биномы, группа перестановок, подгруппы, порожденные биномами, криптографические протоколы.

нечными полями, и вопрос возможности их применения в криптографии, поставленный еще в работе [1]. Удивительным оказывается факт, доказанный в данной работе, что, несмотря на то, что двучлены имеют более сложную форму, чем одночлены, их использование в качестве функций шифрования делает криптографический протокол ненадежным. Возможно, в качестве функций шифрования могут быть использованы композиции перестановочных двучленов.

В работе [2] исследовались перестановочные многочлены в форме $x^r h(x^{(q-1)/d})$ над конечными полями $\mathbb{F}_q$, где $d|(q-1)$, и был получен критерий перестановочного многочлена в такой форме. Этот критерий был впоследствии упрощен в работах [3, 4] до приведенного ниже:

Теорема 1. *Пусть $d, r > 0$, $d|(q-1)$ и $h(x) \in \mathbb{F}_q[x]$.*
Тогда $f(x) = x^r h(x^{(q-1)/d})$ является перестановочным многочленом в $\mathbb{F}_q$ тогда и только тогда, когда выполнены два условия:

(1) $\gcd(r, (q-1)/d) = 1$.

(2) *$x^r h(x)^{(q-1)/d}$ является биекцией над μ_d, где μ_d – множество корней степени d из единицы в конечном поле $\mathbb{F}_q$.*

В случае малых значений d, критерий теоремы 1 является эффективным, т.к. может быть проверен за время $O(d^2 \log p)$.

В работе [2] также было доказано, что всё множество таких многочленов в конечном поле $\mathbb{F}_q$ образует группу, порядок которой приведен ниже:

$$N_{d,q} = d! \left(\frac{q-1}{d}\right)^d \phi\left(\frac{q-1}{d}\right), \tag{1}$$

где $\phi(n)$ – функция Эйлера.

Любой перестановочный двучлен $\alpha x^n + \beta x^m$, где $n < m$, можно представить в виде $x^n h(x^{(q-1)/d})$, где $d = \gcd(q-1, m-n)$ и $h(x) = \alpha + \beta x^{d(m-n)/(q-1)}$. Это значит, что теорема 1 также может быть применена и к двучленам, и, в случае малых значений d, такая проверка является эффективной.

В работе [5] доказано, что, если двучлен $\alpha x^n + \beta x^m$ является перестановочным над простым полем $\mathbb{F}_p$, то $\gcd(m-n, p-1) > \sqrt{p} - 1$, и чего следует, что $d < \sqrt{p} + 1$.

Теорема 2. *Если $x^n + \alpha x^m$ – перестановочный двучлен над простым полем $\mathbb{F}_p$, то $\gcd(m-n, p-1) > \sqrt{p} - 1$.*

Также в работе [5] выдвигается гипотеза, что $d < 2\log p$, проверенная экспериментально для всех значений p до 10000. Перечисленные в данной работе перестановочные двучлены для всех простых конечных полей $\mathbb{F}_p$, где $p < 15000$, также согласуются с этой гипотезой. В случае выполнения гипотезы, задача проверки перестановочности для любого двучлена может быть решена эффективно за время $O(\log^3 p)$, если реализовать критерий теоремы 1.

Многочлены в форме $x^r f(x^{(q-1)/d})$ замкнуты относительно операции композиции для фиксированного d. Из этого следует, что обратный многочлен к перестановочному многочлену в форме $x^r f(x^{(q-1)/d})$ также представим в такой форме, т.к. обратный многочлен принадлежит циклической группе, порожденной данным перестановочным многочленом относительно операции композиции. На основе этого можно сделать вывод, что количество членов в обратном многочлене не превосходит числа d. Эффективный способ вычисления коэффициентов обратного многочлена получен в работе [6] и сложность его составляет $O(d^2 \log p)$.

2. Перечисление перестановочных двучленов

Для исследования свойств перестановочных двучленов достаточно перечислить только нормированные двучлены. Базовый алгоритм перечисления приведен на рис. 1. Проверка свойства перестановочности двучлена может быть осуществлена за $O(q)$ операций с затратами по памяти $O(q)$, путем представления конечного поля как циклической группы. Поэтому общая сложность алгоритма на рис. 1 составляет $O(q^4)$ по времени и $O(q)$ по памяти.

Вход: q – порядок конечного поля
Выход: все перестановочные двучлены вида $x^n + ax^m$, $0 < n < m < q-1$

1: **for all** $m \in [2..q-2]$, $n \in [1..m-1]$ **do**
2: **for all** $a \in \mathbb{F}_q^*$ **do**
3: **if** $x^n + ax^m$ перестановочный двучлен **then**
4: **yield** $x^n + ax^m$
5: **end for**
6: **end for**

Рис. 1. Простейший алгоритм перечисления двучленов.

Данный алгоритм может быть применен на практике для порядков полей до 500. Добавление проверки на основе теоремы 2 и простых проверок $\gcd(n, m, q-1) = 1$ и $\gcd(n-m, q-1) \neq 1$, которые легко могут быть получены из свойства единственности корня перестановочного двучлена, позволяет перечислить двучлены для полей $\mathbb{F}_q$ для $q < 1000$. Эти простые проверки на форму двучлена, т.е. на значение m и n, можно записать в виде функции, приведенной на рис. 2.

1: **function** CanHaveShape(n, m, q)
2: $d \leftarrow \gcd(n-m, q-1)$
3: **if** $\gcd(n, m, q-1) \neq 1$ или $d = 1$ **then**
4: **return** False
5: **if** q – простое и $d \leq \sqrt{q} - 1$ **then**
6: **return** False
7: **return** True
8: **end function**

Рис. 2. Функция проверки формы перестановочного двучлена.

2.1. Перечисление главных представителей орбит

Для перечисления двучленов в полях бóльших порядков можно использовать естественную симметрию, возникающую при подстановке в многочлен перестановочного одночлена. На многочленах можно задать группу преобразований, действие которой представляет подстановку перестановочного одночлена в многочлен и умножение на константу:

Определение 1. *Группа преобразований $G(q)$ множества многочленов $f \in \mathbb{F}_q[x]$:*

(1) $G(q) = \{(a, bx^c) \mid a, b \in \mathbb{F}_q^*,\ c \in \{1 \dots q-2\},\ \gcd(c, q-1) = 1\}$.

(2) *Групповая операция:* $(a_1, b_1 x^{c_1}) \cdot (a_2, b_2 x^{c_2}) = (a_1 a_2, b_1 b_2 x^{c_1 c_2})$.

(3) *Действие на многочлен:* $(a, bx^c) \circ f(x) = af(bx^c)$.

Определение 2. *Назовем орбитой многочлена $f \in \mathbb{F}_q$ множество* $\mathrm{Orb}(f)$*, в элементы которого многочлен f переходит под действием элементов группы $G(q)$ по модулю $x^q - x$:*

$$\begin{aligned}\mathrm{Orb}(f) &= \{\alpha \circ f \bmod (x^q - x) \mid \alpha \in G(q)\} \\ &= \{g \in \mathbb{F}_q \mid g = af(bx^c) \bmod (x^q - x),\ (a, bx^c) \in G(q)\}.\end{aligned}$$

Группа преобразований $G(q)$ разбивает множество многочленов на орбиты. Если многочлен является перестановочным, то и все многочлены из его орбиты также являются перестановочными. Обратное также верно: если многочлен не является перестановочным, то и все многочлены из его орбиты также не являются перестановочными. Поэтому можно рассматривать орбиты многочлена как класс эквивалентности. Для перечисления всех перестановочных многочленов достаточно проверить одного представителя для каждой из орбит, а затем при необходимости перечислить все элементы таких орбит.

Например, для простого поля $\mathbb{F}_{17}$ все множество перестановочных двучленов разбивается на две орбиты с представителями $x+4x^9$ и $x+14x^9$.

Для исследования перестановочных двучленов, как будет показано ниже, достаточно перечисления только одного двучлена из каждой орбиты. Введем полный порядок на двучленах ax^n+bx^m (где $n<m$), соответствующий лексикографическому порядку кортежа (n,m,a,b) с каким-либо порядком на элементах поля $\mathbb{F}_q$, необходимого для сравнения a_1 с a_2 и b_1 с b_2:

Определение 3. *Будем говорить, что* $a_1x^{n_1}+b_1x^{m_1}<a_2x^{n_2}+b_2x^{m_2}$, *где* $n_1<m_1$ *и* $n_2<m_2$, *если* $(n_1,m_1,a_1,b_1)<(n_2,m_2,a_2,b_2)$ *лексикографически.*

Определение 4. *Главным представителем орбиты будем называть минимальный элемент орбиты по введенному порядку.*

Теорема 3. *Пусть* $f(x)=ax^n+bx^m\in\mathbb{F}_q[x]$, *где* $n<m$, *– главный представитель орбиты* $\mathrm{Orb}(f)$. *Тогда* $a=1$ *и* $n|(q-1)$.

Доказательство.

1. Пусть $a\neq 1$. Тогда $a^{-1}f(x)<f(x)$ и $a^{-1}f(x)\in\mathrm{Orb}(f)$. А следовательно, $f(x)$ не является минимальным в орбите.
2. Пусть $\gcd(n,q-1)=n_1\neq n$. Следовательно $\gcd(n/n_1,q-1)=1$. Используя расширенный алгоритм Евклида можно получить α и β:
$$1=\alpha(n/n_1)+\beta(q-1)\Rightarrow\gcd(\alpha,q-1)=1.$$
Рассмотрим подстановку x^α в двучлен $f(x)$:
$$\begin{aligned}f(x^\alpha)&=x^{n\alpha}+bx^{m\alpha}=x^{n_1-n_1\beta(q-1)}+bx^{m\alpha}\\&\equiv x^{n_1}+bx^{m_1}\pmod{x^q-x},\end{aligned}$$

где $m_1 = m\alpha \bmod (q-1)$.

Если $n_1 < m_1$, то $g(x) = (f(x^\alpha) \bmod (x^q - x)) < f(x)$, а следовательно $f(x)$ не является главным представителем.

Если $n_1 > m_1$, то $g(x) = (b^{-1} f(x^\alpha) \bmod (x^q - x)) < f(x)$, а следовательно $f(x)$ также не является главным представителем. □

По теореме 3 в качестве кандидатов на главные представители орбит в алгоритме перебора достаточно проверять двучлены в форме $x^n + ax^m$, где $n < m$, $n < \gcd(m, q-1)$ и $n|(q-1)$.

Следующая теорема 4 позволит добавить дополнительное ограничение на коэффициент a.

Теорема 4. *Пусть $f(x) = x^n + ax^m \in \mathbb{F}_q$ – перестановочный двучлен. Пусть $d = (q-1)/\gcd(m-n, q-1)$. Тогда $g(x) = x^n + bx^m$ принадлежит орбите многочлена f тогда и только тогда, когда:*

(i) *$ab^{-1} \in \mu_d$ или $ab \in \mu_d$, если $\exists c \in \mathbb{N} : \begin{cases} c^2 = 1 \mod (q-1) \\ n = c \cdot m \mod (q-1) \end{cases}$;*

(ii) *$ab^{-1} \in \mu_d$, иначе.*

где μ_d – множество корней из единицы степени d.

Доказательство. Если $ab^{-1} \in \mu_d$, то существует подстановка и умножение на константу, переводящие $f(x)$ в $g(x)$. В случае если условие существования c из пункта (i) выполнено, то подстановка в многочлен $f(x)$ монома cx и умножение на константу $a^{-1}c^{-m}$ переводит многочлен $f(x)$ в многочлен $x^m + a^{-1}c^{n-m}x^n$. Если $ab \in \mu_d$, то этот двучлен может быть аналогично переведен в двучлен $g(x)$. Подробное рассмотрение данных случаев приводит к требуемому доказательству. □

По теореме 4 в качестве коэффициента a для кандидатов на главные представители орбит в алгоритме перебора достаточно проверять элементы из факторгруппы $\mathbb{F}_q^*/\mu_d$, где $d = (q-1)/\gcd(m-n, q-1)$. В случае, если условие (ii) теоремы 4 выполняется, то также следует проверить, что $a = \min(a, a^{-1})$.

На основании теорем 3 и 4 в данной работе был построен алгоритм 3, перечисляющий главных представителей орбит перестановочных двучленов.

Сложность алгоритма 3 по времени составляет $O(q^3\tau(q))$, где $\tau(q)$ – количество делителей числа q. В книге [7, стр. 296] доказано, что $\tau(q) = o(n^\epsilon)$ для любого $\epsilon > 0$. Поэтому общая сложность по времени

составляет $O(n^{3+\epsilon})$. Сложности по памяти составляет $O(q)$. Следует отметить, что данный алгоритм перечисляет орбиты по одному разу, т.к. главный представитель в орбите единственен, а поэтому проверка на то, что двучлен принадлежит орбите другого обработанного двучлена, не требуется.

Описанный алгоритм на рис. 3 позволил перечислить всех главных представителей орбит перестановочных двучленов для конечных полей $\mathbb{F}_q$ для всех $q < 15000$. В приложении А приведены значения количества орбит перестановочных двучленов вместе с общим количеством перестановочных двучленов для некоторых порядков конечных полей.

Вход: q – порядок конечного поля

Выход: все главные представители орбит перестановочных двучленов

for all $n \in [1..m-1]$ **do**
  if $\gcd(n, q-1) \neq n$ **then**
    continue
  for all $m \in [2..q-2]$ **do**
    if $n > \gcd(m, q-1)$ или CanHaveShape (n, m, q) = False **then**
      continue
    $d \leftarrow (q-1)/\gcd(q-1, m-n)$
    if $\exists c \in \mathbb{N} : c^2 = 1 \bmod (q-1), n = c \cdot m \bmod (q-1)$ **then**
      if $a \neq \min(a, a^{-1})$ **then**
        continue
      for all $a \in \mathbb{F}_q^*/\mu_d$ **do**
        if $x^n + ax^m$ – перестановочный двучлен **then**
          yield $x^n + ax^m$
      end for
  end for
end for

Рис. 3. Перечисление главных представителей орбит перестановочных двучленов.

Анализ результатов перечисления орбит эквивалентности показал, что подавляющее большинство представителей имеют форму

$x(1 + bx^r)$. Это значит, что для большинства перестановочных двучленов $ax^n + bx^m$ либо $\gcd(n, q-1) = 1$, либо $\gcd(m, q-1) = 1$. Количество представителей, которые не могут быть записаны в таком виде, составляет 0.15%, а количество перестановочных двучленов, соответствующих таким представителям, составляет 0.3% от общего количества перестановочных двучленов.

2.2. Размер орбиты

Для вычисления общего количества перестановочных двучленов необходимо знать размер орбиты. Для этого вначале рассмотрим общий случай: пусть $f(x)$ – многочлен над $\mathbb{F}_q$. Обозначим через H_f подгруппу группы $G(q)$ (см. определение 1), переводящую многочлен f сам в себя по модулю $x^q - x$:

$$H_f = \{x \in G(q) \mid x \circ f \equiv f \bmod (x^q - x)\}. \tag{2}$$

Введенная подгруппа H_f является нормальной, т.к. группа $G(q)$ является абелевой. Факторгруппа $G(q)/H_f$ является группой, задающей преобразование многочлена f в элементы орбиты многочлены f без повторений. Поэтому количество N_f многочленов орбиты можно вычислить следующим образом:

$$N_f = |G/H_f| = \frac{|G|}{|H_f|} = \frac{(q-1)^2\phi(q-1)}{|H_f|}, \tag{3}$$

где $\phi(x)$ – функция Эйлера, равная количеству чисел, взаимно простых с x и меньших x.

Для перестановочного двучлена f размер группы H_f может быть вычислен по следующей теореме:

Теорема 5. *Пусть $f(x) = x^n + bx^m$ – невырожденный перестановочный двучлен над $\mathbb{F}_q$, т.е. $n \neq m$ и $b, m, n \neq 0$. Пусть $d = (q-1)/\gcd(m-n, q-1)$.*

Тогда $|H_f| = \gamma \cdot \gcd(m-n, q-1)$, где $\gamma \in \{1, 2\}$. $\gamma = 2$ при выполнении двух условий:

(i) $\exists c \in \mathbb{N} : \begin{cases} c^2 = 1 \mod (q-1) \\ n = c \cdot m \mod (q-1) \end{cases}$;

(ii) $b^2 \in \mu_d$.

Во всех остальных случаях $\gamma = 1$.

Доказательство. Аналогично доказательству теоремы 4 в случае существования c и $b^2 \in \mu_d$ существует подстановка, переводящая

двучлен $f(x)$ сам в себя, при котором моном x^n переходит в x^m и наоборот. Детальное рассмотрение всех возможных подстановок, переводящих $f(x)$ в $f(x)$ приводит к требуемому доказательству. $\square$

Общее количество двучленов в орбите может быть вычислено по формуле (3) и теореме 5:

$$N_f = |G/H_f| = \frac{|G|}{|H_f|} = \frac{(q-1)^2\phi(q-1)}{\gamma \cdot \gcd(m-n, q-1)}, \tag{4}$$

где $\gamma \in \{1, 2\}$ определяется условием теоремы 5.

На основе результатов перечисления представителей орбит и формулы (4) для размера орбиты можно вычислить общее количество перестановочных двучленов в конечном поле $\mathbb{F}_q$:

$$N_q = \sum_{f_i \in C} \frac{(q-1)^2\phi(q-1)}{\gamma_i \cdot \gcd(m_i - n_i, q-1)}, \tag{5}$$

где $C = \{f_i\}$ – представители перестановочных орбит, а $\gamma_i \in \{1, 2\}$ определяется условием теоремы 5 для каждого перестановочного двучлена f_i.

Количество $\widetilde{N}_q$ перестановочных двучленов с нормированным старшим коэффициентом может быть вычислено как

$$\widetilde{N}_q = \frac{N_q}{q-1}. \tag{6}$$

По формуле (6) было вычислено количество перестановочных двучленов для всех обработанных порядков полей. Зависимость количества от порядка поля приведена на рис. 5, а численные значения для некоторых порядков приведены в приложении А.

Анализ результатов показывает, что количество перестановочных двучленов для простых полей $\mathbb{F}_q$ меньше, чем для полей $\mathbb{F}p^n$, где $n > 1$, при сравнимом порядке поля. Например, количество нормированных перестановочных двучленов для $\mathbb{F}_{2^{14}}$ равно 515×10^6 (данный результат не приведен на графике), а количество для $\mathbb{F}_p$ при $p \approx 2^{14} = 16384$ не больше 75×10^6.

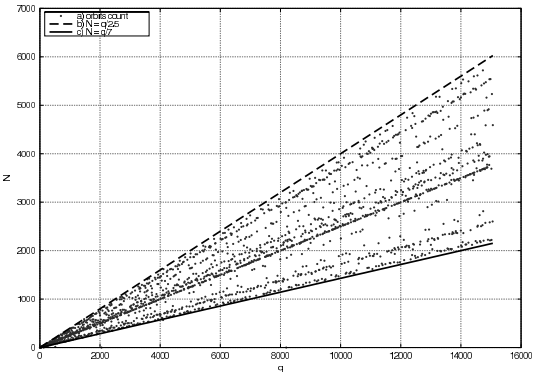

Рис. 4. Количество перестановочных орбит в зависимости от q.

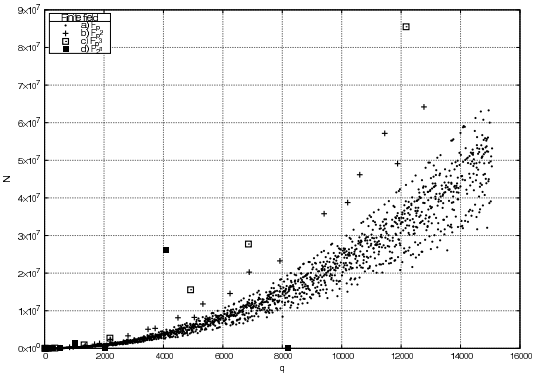

Рис. 5. Количество перестановочных двучленов с нормированным старшим коэффициентом в зависимости от q.

3. Группы, порожденные перестановочными двучленами

Замыкание всего множества двучленов относительно операции композиции представляет собой группу, элементы которой являются функциями, представимыми в виде композиции перестановочных двучленов. Порядок такой группы равен количеству таких функций.

Для исследования порядков групп, порожденных перестановочными двучленами, использовалась система компьютерной алгебры GAP. Для вычисления порядка группы в качестве образующих группы использовались главные представители орбит двучленов и перестановочные одночлены, т.к. любой перестановочный двучлен

Таблица 1. Количество перестановочных двучленов с нормированным старшим коэффициентом и количество орбит над полем $\mathbb{F}_q$ для некоторых q, где $C-$ количество классов перестановочных двучленов, $N-$ количество перестановочных двучленов

q	C	N
7	1	4
8	0	0
9	0	0
11	2	16
13	1	8
16	1	40
17	2	24
19	5	66
23	5	100
...	...	...
4931	1339	5383168
4933	1223	5414976
4937	729	4206048
4943	1251	5453184
4951	1698	4899600
4957	1438	5657088
4967	1241	5658960
...	...	...
14947	5538	63273184
14951	3946	44980320
14957	2584	49326648
14969	2211	38619240
14983	5540	60021080
15013	3690	49714776
15017	2221	39073328
...	...	...
16384	1963	515980584

представим в виде композиции главного двучлена и одночлена.

Система GAP позволила просчитать порядки групп перестановочных двучленов над конечными полями $\mathbb{F}_q$, порядки которых не превосходят 500. Результаты для некоторых значений q приведены в таблице 2.

Таблица 2. Порядки групп, порожденных перестановочными двучленами

q	порядок группы $B(q)$	d
29	345744	7
31	30!	1
41	6400	20
47	23276	23
59	47096	29
61	60!	1
73	1042682221795737600	6

Оказалось, что для всех значений q кроме 73 порядок группы, порожденной всеми перестановочными двучленами $\{x^{n_i} + a_i x^{m_i}\}$ совпадает с порядком группы, порожденной перестановочными многочленами в форме $x^r h(x^{(q-1)/d})$, где

$$d = (q-1)/\gcd(q-1, m_1 - n_1, m_2 - n_2, \dots).$$

Обозначим через $B(q)$ группу, порожденную перестановочными двучленами, а через $G(d,q)$ – группу, порожденную многочленами в форме $x^r h(x^{(q-1)/d})$. Многочлены группы $G(d,q)$, как уже было сказано во введении, исследовались в работе [2]. Порядок группы $G(d,q)$ вычисляется по формуле (7).

$$|G(d,q)| = d! \left(\frac{q-1}{d}\right)^d \phi\left(\frac{q-1}{d}\right), \tag{7}$$

где $\phi(n)$ – функция Эйлера.

Группа $B(q)$ является подгруппой группы $G(d,q)$. Следовательно, в случае, когда порядки этих групп совпадают, группы равны. Поэтому для проверенных $q < 500$, $q \neq 73$ группы $B(q)$ совпадает с $G(d,q)$. Это значит, что любой перестановочный многочлен в форме $x^r h(x^{(q-1)/d})$ может быть выражен через композицию перестановочных двучленов $x^n + ax^m$ при $d = (q-1)/\gcd(q-1, m-n)$. Данное предположение сформулировано в виде гипотезы 1.

Гипотеза 1. *Почти все (за исключением конечного числа) многочлены в форме $x^r h(x^{(q-1)/d})$ над конечными полями $\mathbb{F}_q$ представимы*

в виде композиции перестановочных двучленов $x^n + ax^m$, *для которых* $(q-1)/\gcd(q-1, m-n) = d$.

Также экспериментальные результаты показали, что для некоторых конечных полей $\mathbb{F}_q$ порядок группы $B(q)$ равен $(q-1)!$. Это значит, что в таких полях любая биекция, переводящая 0 в 0, может быть представлена как композиция перестановочных двучленов. Данное предположение сформулировано в виде гипотезы 2.

Гипотеза 2. *Существует бесконечное числа конечных полей, в которых любая биективная функция* $f(x)$, *с условием* $f(0) = 0$, *представима в виде композиции перестановочных двучленов.*

В системе GAP было проверено, что гипотеза 2 выполняется для конечных полей, некоторые порядки которых равны 31, 61, 64,..., 4096, 4489 и 4621. Данное утверждение можно записать, как теорему 6, которая доказана экспериментально.

Теорема 6. *Пусть* $q \in \{31, 61, 64, 211, 256, 421, 841, 1024, 1331, 1849, 2521, 2809, 3125, 3481, 3721, 4096, 4489, 4621\}$.

Тогда выполнены следующие два утверждения:

- *Любая биективная функция* f *в поле* $\mathbb{F}_q$ *представима в виде композиции двучленов, при условии* $f(0) = 0$.
- *Перестановочные двучлены порождают симметрическую группу* S_{q-1} *относительно операции композиции.*

4. Построение случайных перестановочных двучленов

Теорема 1 позволяет построить эффективный алгоритм проверки перестановочности двучлена в форме $x^n + ax^m$ при малых значениях $d = (q-1)/\gcd(q-1, m-n)$. Поэтому строить случайные перестановочные двучлены можно, проверяя этот критерий перестановочности для случайных двучленов $x^n + ax^m$. Наилучшая оценка количества значений a, при которых такой двучлен является перестановочным, получена в работе [5]:

$$\begin{aligned} &- d!\left(\frac{2}{d^d} + (d-2) - \frac{2}{d}\right)\sqrt{q} - d!\frac{d+1}{d^d} \\ &\leq \left(N - \frac{d!}{d^d}(q+1)\right) \leq d!\left(\frac{2}{d^d} + (d-2) - \frac{2}{d}\right)\sqrt{q}. \end{aligned} \tag{8}$$

Из оценки по формуле (8) следует, что алгоритм, проверяющий случайные перестановочные двучлены при фиксированном значении n и m, в среднем сделает $d^d/d!$ шагов. Такой алгоритм был реализован, и, несмотря на большую теоретическую погрешность оценки в формуле (8), он позволяет строить случайные перестановочные двучлены при малых значениях d.

В таблице 3 приведены результаты эксперимента, в котором строились случайные перестановочные двучлены при $d = 2, 4, 8$ и 16. Из результатов видно, что построение таких двучленов на практике реализуемо для $d < 10$, а при $d = 16$ построить перестановочный двучлен не удалось.

Таблица 3. Количество шагов при поиске случайного перестановочного двучлена. Исследовалось в простом поле $\mathbb{F}_p$, где $p \approx 10^{20}$. Количество построенных перестановочных двучленов равно 2000. В столбце σ указано среднеквадратическое отклонение

Форма	$\frac{d^d}{d!}$	Среднее количество шагов	σ
$x(\alpha + x^{(p-1)/2})$	2.00	2.04	1.71
$x(\alpha + x^{(p-1)/4})$	10,66	10.40	13.64
$x(\alpha + x^{(p-1)/8})$	416.10	411.70	587.73
$x(\alpha + x^{(p-1)/16})$	881658.00	—	—

На сегодняшний день не существует алгоритма, который позволял бы строить произвольные случайные перестановочные двучлены при больших значениях d. Но при, например, $d = 4$ построение такого двучлена занимает малое время и может быть реализовано на практике.

5. Обобщение RSA с использованием двучленов

Для построения произвольного перестановочного многочлена $h(x)$ над кольцом $\mathbb{Z}/pq\mathbb{Z}$, где p и q являются простыми числами, можно построить перестановочные многочлены $f(x)$ и $g(x)$ полях $\mathbb{F}_p$ и $\mathbb{F}_q$, а затем по китайской теореме об остатках восстановить многочлен $h(x)$, удовлетворяющий условиям $h(x) \equiv f(x) \pmod{p, x^p - x}$ и $h(x) \equiv g(x) \pmod{q, x^q - x}$. В общем случае такой многочлен будет плотным,

и при больших значениях p и q не может быть вычислен на практике. Но при специальном выборе формы чисел p и q и специальном выборе двучленов $f(x)$ и $g(x)$, многочлен $h(x)$ будет двучленом. Например, если $p = 149$ и $q = 317$, а $f(x) = x^{38} + 92x$ и $g(x) = x^{238} + 85x$, то многочлен $h(x)$ будет перестановочным двучленом в кольце $\mathbb{Z}/pq\mathbb{Z}$ и $h(x) = x^{8770} + 37491x$.

Эффективный способ обращения двучленов в конечных полях при малых значениях d был найден в работе [6]. Но основании этого можно было бы использовать для обобщения криптографического протокола RSA двучлен $h(x)$ в качестве публичной функции шифрования, а для расшифровки можно вычислять $f^{-1}(x)$ и $g^{-1}(x)$ и применять китайскую теорему об остатках.

Криптостойкость протокола RSA основа на сложности факторизации чисел. Существуют алгоритмы факторизации, использующие свойства делителей факторизуемого числа. Так, например, если p является делителем числа n, и все делители $p-1$ являются малыми числами, то для факторизации n может быть применен $p-1$ метод Полларда [8]. Традиционной рекомендацией для создания стойкого криптографического ключа для RSA является использование сильных простых чисел. Но в 1999 году Ривест и Сильверман в работе [9] проанализировали сложность задачи факторизации чисел и пришли к выводу, что рекомендация использования сильных простых чисел не является обязательной.

Определение 5. *Число p называется сильным простым числом, если $p = ap' + 1$, где p' – большое простое число, а $a < \log p$*

В самой работе [9] приводится более полное определение, учитывающие, что число p' также является сильным простым, а также $p+1$ имеет большой простой делитель. Для данной же работы более слабое определение является достаточным. В работе [9] в качестве верхней границы для числа a указывается 2^{12}. Будем считать, что $a < \log p$, как и указано в определении.

Считается, что если p и q являются сильными простыми числами, то задача факторизации pq является более сложной, чем для общего случая p и q. Но оказывается, что если в качестве функции шифрования использовать двучлен, то из-за свойств перестаночных двучленов такой криптографический протокол является ненадежным при любом выборе шифрующего двучлена.

Теорема 7. *Пусть $h(x) = ax^s + bx^m$ – перестановочный двучлен в*

кольце $\mathbb{Z}_n/pq\mathbb{Z}$, где p и q – сильные простые числа. Тогда значения p и q могут быть вычислены, зная $h(x)$ и n, за время $O(\log^6 n)$.

Доказательство. Пусть

$$f(x) = h(x) \pmod{p, x^p - x} = a_1 x^{s_1} + b_1 x^{m_1}.$$

$f(x)$ является перестановочным двучленом в простом поле $\mathbb{F}_p$.

$\frac{p-1}{\gcd(s_1-m_1,p-1)} < \sqrt{p}$, по теореме 2. Но $s_1 - m_1 \equiv s - m \pmod{p-1}$. Значит

$$\frac{p-1}{\gcd(s-m,p-1)} < \sqrt{p}. \tag{9}$$

Число p являются сильным простым числом, а следовательно, $p - 1 = cp'$, где p' – простое и $c < \log p$. Значит из формулы (9) следует, что p' является делителем $s - m$.

Аналогично можно доказать, что число q' является делителем $s-m$, где $q - 1 = dq'$, q' – простое, а $d < \log q$.

1. Если $p' = q'$, то $n = pq = (cp' + 1)(dq' + 1) = cdp'^2 + (c + d)p' + 1$. Простой перебор всех значений c и d до $\log n$, позволяет найти p', а следовательно, и p за время $O(\log^4 n)$.
2. Пусть $p' \neq q'$.
$\frac{s-m}{p'q'} \leq cd < \log^2 n$.

Значит существуют числа $\alpha, \beta < \log^2 n$, что $\alpha(s - m)/\beta = (p - 1)(q - 1)$, т.к. $s - m < pq$. Для каждого $\alpha, \beta < \log^2$ можно попробовать решить систему (10):

$$\begin{cases} pq = n, \\ \alpha(s-m)/\beta = (p-1)(q-1) \end{cases} \tag{10}$$

относительно p и q в обычной целочисленной арифметике. По исходному предположения существует α, $\beta < \log^2 n$, при которых система имеет решение, а значит перебором всех таких значений α и β решение системы может быть найдено за время $O(\log^6 n)$.

Следовательно, за $O(\log^6 n)$ операций задача факторизации может быть осуществлена, если известен перестановочный двучлен. □

Доказательство теоремы 7 является конструктивным. При условии $p' \neq q'$ алгоритм приведен на рис. 6. Для случая $p' = q'$ алгоритм

также может быть реализован, но такие числа не используются в RSA из-за простоты факторизации даже без знания $f(x)$.

Вход: s, m – степени двучлена $ax^s + bx^m$, n – произведение p и q.

Выход: p и q.

1: **for all** $\alpha \in [1..\log^2 n]$, $\beta \in [1..\log^2 n]$ **do**
2: $s \leftarrow \frac{\alpha(s-m)}{\beta}$
3: **if** s не является целым **then**
4: **continue**
5: $q \leftarrow \frac{(n-s+1)\pm\sqrt{(n-s+1)^2-4n}}{2}$
6: **if** q не является целым **then**
7: **continue**
8: **if** $n \bmod q' = 0$ **then**
9: **return** $(q', n/q')$
10: **end for**

Рис. 6. Алгоритм взлома модельного криптографического протокола.

Как уже было сказано, сложность вскрытия криптографического протокола RSA основывается на сложности факторизации числа $n = pq$. В случае с перестановочными двучленами $ax^s + bx^m$ найти разложение n на множители можно также и путем разложения $m - s$ на множители. Почти все делителей чисел $p-1$ и $q-1$ будут также делителями $m - s$, а значит, зная разложение $m - s$ можно применить $p-1$ метод Полларда к числу n, но с заведомо известным набором делителей чисел $p-1$ и $q-1$. Это значит, что криптостойкость такого модельного криптографического протокола основана на сложности задачи факторизации числа $n = pq$ и числа $s - m$, при условии, что $s - m$ имеет большое число общих делителей с $p-1$ и $q-1$.

Если числа p и q не являются сильными простыми числами, то приведенный выше алгоритм также работает корректно, но в предположении справедливости гипотезы $d < 2\log p$, высказанной в работе [5] и упомянутой в начале данной статьи.

Из приведенных выше рассуждения и доказательств следует, что схема шифрования, использующая перестановочные двучлены, оказывается не надежной. Хотя форма перестановочных двучленов сложнее формы одночлена, двучлены не могут быть использованы в качестве функции шифрования по модулю составного числа, ввиду слабой

криптостойкости такой схемы из-за особой структуры перестановочных двучленов. Тем не менее, более сложные перестановочные многочлены, например, трехчлены, могут не обладать такой структурой.

6. Заключение

В первой части данной работы на основе разработанного метода были перечислены все главные представители орбит перестановочных двучленов для порядков полей до 15000 включительно. Была доказана формула размеры орбиты, на основе которой было вычислено количество перестановочных двучленов для исследованных полей. Интересным результатом являются обнаруженные порядки конечных полей, в которых перестановочные двучлены порождают все биективные функции со значением 0 в 0, а также равенство группы, порожденной перестановочным двучленами, и группы, порожденной многочленами вида $x^r f(x^{(q-1)/d})$, для всех исследованных порядков полей, кроме одного значения $q = 73$.

Во второй части работы вначале был показано, что можно строить перестановочные двучлены над конечными полями и на основе этого было показано, что можно построить модельный криптографический протокол с использованием двучленов в качестве шифрующих функций, аналогичный криптографическому протоколу RSA. Но из-за свойств перестановочных двучленов было доказано, что использование двучленов в качестве функций шифрования делает протокол ненадежным. Вопрос о возможности использования в качестве функции шифрования более сложных многочленов, например трехчленов, остается открытым.

Литература

1. R. Lidl, G. L. Mullen, *When does a polynomial over a finite field permute the elements of the field?* — The American Mathematical Monthly **95** (1988), 243. http://www.jstor.org/stable/2323626?origin=crossref.
2. D. Wan, R. Lidl, *Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure?* — Monatshefte für Mathematik **112** (1991), 149. http://www.springerlink.com/content/x840551169017000/.
3. A. Akbary, Q. Wang, *On polynomials of the form $x^r f(x^{(q-1)/l})$* — International Journal of Mathematics and Mathematical Sciences (2007), 1. http://www.hindawi.com/journals/ijmms/2007/023408.abs.html.
4. M. E. Zieve, *On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{((q-1)/d)})$*, ArXiv e-prints, http://arxiv.org/abs/0707.1110 (2007).
5. A. M. Masuda, M. E. Zieve, *Permutation binomials over finite fields*, ArXiv e-prints, http://arxiv.org/abs/0707.1108 (2007).

6. Q. Wang, *On inverse permutation polynomials* — Finite Fields and Their Applications **15** (2007), 12.
http://linkinghub.elsevier.com/retrieve/pii/S1071579708000750.
7. T. M. Apostol, *Introduction to Analytic Number Theory*. Springer, 1976.
8. J. M. Pollard, *Theorems on factorization and primality testing* — Mathematical Proceedings of the Cambridge Philosophical Society **76** (1974), 521.
http://www.journals.cambridge.org/abstract_S0305004100049252.
9. R. L. Rivest, R. D. Silverman, *Are 'Strong' Primes Needed for RSA?* — in: In The 1997 RSA Laboratories Seminar Series, Seminars Proceedings (1999). *http://eprint.iacr.org/2001/007*.

Vasiliev N. N., Rybalkin M. A. Permutation binomials and their groups.

This paper is devoted to studying properties of permutation binomials over finite fields and studying possibility to use permutation binomials as enryption function. We present permutation binomials enumeratation algorithm. Using this algorithm all permutation binomials for finite field up to order 15000 were generated. Using this data we investigate groups, generated by permutation binomials and found that over some finite fields $\mathbb{F}_q$ every bijective function over $[1..q-1]$ can be represented as composition of binomials. We study possibility of permutaion binomials generation over large prime fields. And we prooved that RSA generalization using permutation binomials isn't secure.

С.-Петербургское отделение
Математического института
им. В.А.Стеклова РАН, Фонтанка 27,
191023 Санкт-Петербург, Россия

E-mail: vasiliev@pdmi.ras.ru
michael.rybalkin@gmail.com

Поступило 21 декабря 2010 г.