Национальная академия наук Беларуси
Труды Института математики НАН Беларуси. 2024. Том 32. № 2. С. 7–16

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ
ALGEBRA AND NUMBER THEORY

УДК 512.71

ФУНДАМЕНТАЛЬНАЯ ОБЛАСТЬ В СПЕЦИАЛЬНОЙ ЛИНЕЙНОЙ ГРУППЕ $SL_2(\mathbb{F}_p[x])$ И СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА НА ЕЕ ОСНОВЕ

Г. В. Матвеев[1], **А. А. Осиновская**[2], **В. И. Янчевский**[2]

[1]*Белорусский государственный университет, Минск, Беларусь*
[2]*Институт математики НАН Беларуси, Минск, Беларусь*
e-mail: matveev47@bsu.by, anna@im.bas-net.by, yanch@im.bas-net.by

Поступила: 16.10.2024 **Исправлена:** 23.11.2024 **Принята:** 12.12.2024

Ключевые слова: специальная линейная группа, конгруэнц-подгруппа, фундаментальная область, модулярное разделение секрета, пороговая структура доступа.

Аннотация. Решается задача по разработке математических основ модулярного разделения секрета в специальной линейной группе над кольцом многочленов от одной переменной над конечным полем Галуа из p элементов. К схемам разделения секрета предъявляется большое число требований: совершенность и идеальность схемы, возможность проведения верификации, изменение порога без участия дилера, реализация непороговой структуры доступа и некоторые другие. Каждая разработанная к настоящему времени схема разделения секрета не в полной мере удовлетворяет всем этим требованиям. Разработка схемы на новой математической основе призвана расширить список этих конфигураций, что создает для пользователя больше возможностей в выборе оптимального варианта. В специальной линейной группе размерности 2 над кольцом многочленов строится фундаментальная область относительно действия главной конгруэнц-подгруппы правыми сдвигами. На этой основе предложены способы модулярного порогового разделения секрета и его восстановления.

A FUNDAMENTAL DOMAIN IN THE SPECIAL LINEAR GROUP $SL_2(\mathbb{F}_p[x])$ AND SECRET SHARING ON ITS BASIS

G. V. Matveev[1], **A. A. Osinovskaya**[2], **V. I. Yanchevskiĭ**[2]

[1]*Belarusian State University, Minsk, Belarus*
[2]*Institute of Mathematics of the National Academy of Sciences of Belarus, Minsk, Belarus*
e-mail: matveev47@bsu.by, anna@im.bas-net.by, yanch@im.bas-net.by

Received: 16.10.2024 **Revised:** 23.11.2024 **Accepted:** 12.12.2024

Keywords: a special linear group, a congruence subgroup, a fundamental domain, modular secret sharing, a threshold access structure.

Abstract. The problem of developing the mathematical foundations of modular secret sharing in the special linear group over the ring of polynomials in one variable over the finite Galois field with p elements is being solved. Secret sharing schemes should meet a large number of requirements: perfectness and ideality of a scheme, possibility of verification, changing a threshold without participation of a dealer, implementation of a non-threshold access structure and some others. Every secret sharing scheme developed to date does not fully satisfy all these requirements. The development of a scheme on a new mathematical basis is intended to expand the list of these configurations, thereby creating more possibilities for a user to choose the optimal option. A fundamental domain with respect to the action of the main congruence subgroup by right shifts in the special linear group of dimension 2 over the ring of polynomials is constructed. On this basis, methods for modular threshold secret sharing and its reconstruction are proposed.

1. Введение

В последнее время все большее значение приобретает организация схем доступа к тем или иным информационным ресурсам. Подобного рода задачи призваны решать схемы разделения секрета, относящиеся к числу важных криптографических протоколов. Они используются в системах электронного голосования [1], шифрования на основе атрибутов [2] и в распределенных конфиденциальных вычислениях [3].

Схема разделения секрета решает следующую задачу. Пусть имеется некоторая важная информация (секрет) s и множество $P = \{1, 2, \ldots, k\}$ пользователей. Требуется сообщить каждому пользователю i некоторую информацию s_i (частичный секрет) таким образом, чтобы только заранее определенные группы участников могли, объединяя свои частичные секреты, восстановить секрет s, а для остальных групп эта задача являлась бы трудноразрешимой. Как правило, под этим понимается, что задача восстановления секрета неразрешенной группой участников должна быть эквивалентна полному перебору.

Настоящая работа посвящена модулярному подходу в теории разделения секрета. Основы этого подхода и теории в целом были заложены в работе А. Шамира [4], а собственно модулярный подход получил развитие в работах К. Асмута и Дж. Блума [5] и М. Миньотта [6].

В дальнейшем модулярный подход был развит в работах [7–9]. В частности, он был обобщен на кольца многочленов от одной и нескольких переменных над полем Галуа. Было показано, что любая структура доступа допускает модулярную реализацию в кольцах целых чисел и многочленов над полями Галуа. В работе [7] было доказано, что модулярный подход в кольце многочленов от одной переменной над полем Галуа позволяет реализовать пороговую структуру доступа совершенно и идеально. Более того, модулярная пороговая схема в кольце многочленов от одной переменной над полем Галуа легла в основу стандарта Республики Беларусь 12.34.101.60–2014 «Информационные технологии и безопасность. Алгоритмы разделения секрета». В работах [10; 11] были предложены методы верификации модулярных схем.

В настоящее время для схем разделения секрета разработано много критериев качества, таких как совершенность, идеальность, верифицируемость, пригодность для реализации предпороговых структур доступа и ряд других. Схем разделения секрета, удовлетворяющих всем известным критериям качества, еще нет. Вот почему представляет интерес построение новых схем, основанных на принципиально иной алгебраической базе. В настоящей работе в качестве такой базы предлагается специальная линейная группа над кольцом многочленов от одной переменной над полем Галуа и модулярное разделение секрета в ней.

2. Модулярное разделение секрета

Определение 2.1. Под структурой доступа Γ множества $P = \{1, 2, \ldots, k\}$ пользователей понимают монотонное семейство подмножеств, т. е. семейство, для элементов которого выполняется условие

$$A \in \Gamma,\ A \subset B \subset P \Rightarrow B \in \Gamma.$$

Эти подмножества называют разрешенными, а остальные – запрещенными. Под реализацией структуры доступа будем понимать построение соответствующей схемы разделения секрета.

Структура доступа, когда разрешенными считаются подмножества A с условием $|A| \geqslant t$, называется (t, k)-*пороговой*, а число t, $1 \leqslant t \leqslant k$, называется ее *порогом*.

Схемой разделения секрета (СРС) называют алгоритмы распределения частичных секретов и восстановления исходного секрета. Они, в частности, должны обеспечивать правильное восстановление секрета разрешенными группами участников. Схему разделения секрета называют *совершенной*, если запрещенное множество участников не получает никакой информации о секрете, кроме априорной.

Схему разделения секрета называют *идеальной*, если ключи всех участников и ключ s имеют один и тот же размер. Иногда в условие идеальности включают и совершенство схемы.

В самых общих чертах СРС позволяет распределить секрет между t участниками таким образом, чтобы заданные разрешенные множества участников могли однозначно восстановить

секрет, а неразрешенные – не получили бы никакой дополнительной к имеющейся априорной информации о возможном значении секрета.

Модулярное разделение секрета основано на следующем простом наблюдении (схема Миньотта [6]). Пусть $m_1 < m_2 < \ldots < m_k$ – система попарно взаимно простых натуральных модулей. Если секретом является некоторое натуральное число s, а секретом i-го участника, $i \in P = \{1,2,..,k\}$, является наименьший неотрицательный вычет s по модулю m_i, т. е. $s_i \equiv s \pmod{m_i}$, то группа участников $A \subset P$ восстанавливает исходный секрет s путем решения системы сравнений $x \equiv \equiv s_i \pmod{m_i}$, $i \in A$. Это можно сделать, например, с помощью китайской теоремы об остатках. При этом правильно найдет секрет s лишь та группа участников A, для которой выполнено условие $s < \prod\limits_{i \in A} m_i$. Тот же принцип используется при построении схемы разделения секрета над кольцом многочленов от одной и нескольких переменных [7–9].

Замечание. В схеме Асмута–Блума [5] пользователи находят вспомогательный секрет как указано выше. Хранимым секретом является вычет вспомогательного по некоторому несекретному модулю m_0.

3. Фундаментальная область в специальной линейной группе

Целью статьи является построение модулярной схемы разделения секрета в специальной линейной группе $SL_2(\mathbb{F}_p[x])$, где SL_2 – множество квадратных матриц размерности 2 с определителем 1, $\mathbb{F}_p[x]$ – кольцо многочленов от одной переменной над конечным полем $\mathbb{F}_p$. Мы хотим найти в этой группе все необходимое для построения схем подобно тому, как это происходит в кольце целых чисел $\mathbb{Z}$ [5; 6], в кольце многочленов $\mathbb{F}_p[x]$ [7–9] и в группе $SL_2(\mathbb{Z})$ [12].

Кольцо $\mathbb{F}_p[x]$ имеет много общих свойств с кольцом целых чисел $\mathbb{Z}$ (см. [13, глава 1]). Оба кольца являются областями главных идеалов, оба имеют конечную группу единиц, и оба обладают тем свойством, что у каждого кольца класс вычетов по модулю ненулевого идеала имеет конечное число элементов. Обратимые элементы $\mathbb{F}_p[x]$ – это в точности ненулевые константы (элементы $\mathbb{F}_p^*$). Кольцо $\mathbb{F}_p[x]$, как и $\mathbb{Z}$, является евклидовым, при этом евклидова норма – это степень многочлена deg, т. е. для любых двух многочленов $f(x), g(x) \in \mathbb{F}_p[x]$, $g(x) \neq 0$, имеется однозначное представление в виде $f(x) = g(x)q(x) + r(x)$, для которого $\deg r(x) < \deg g(x)$ или $r(x) = 0$.

Напомним, что в евклидовом кольце каждый необратимый элемент представим в виде конечного произведения простых элементов, и притом однозначно (с точностью до их перестановки и умножения на обратимые элементы). Многочлен $f(x)$ называется нормированным, если его старший коэффициент равен 1. Как и в кольце целых чисел, в кольце многочленов справедлива следующая лемма [13, предложение 1.4], называемая иначе китайской теоремой об остатках.

Лемма 3.1. *Пусть многочлены $f_1(x)$, $f_2(x)$, …, $f_r(x) \in \mathbb{F}_p[x]$ – попарно взаимно просты, $f(x) = f_1(x)f_2(x)\ldots f_r(x)$ и $\varphi_i : \mathbb{F}_p[x]/(f(x)) \to \mathbb{F}_p[x]/(f_i(x))$ – естественные гомоморфизмы. Тогда отображение*

$$\varphi : \mathbb{F}_p[x]/(f(x)) \to \mathbb{F}_p[x]/(f_1(x)) \times \ldots \times \mathbb{F}_p[x]/(f_r(x)), \text{ где для } a \in \mathbb{F}_p[x]/(f(x))$$

$$a \mapsto (\varphi_1(a), \varphi_2(a), \ldots, \varphi_r(a)),$$

является изоморфизмом колец.

Возьмем некоторый многочлен $m(x) \in \mathbb{F}_p[x]$ ненулевой степени. Многочлены $f(x)$ и $g(x)$ сравнимы по модулю $m(x)$ (что записывается $f(x) \equiv g(x) \pmod{m(x)}$), если их остатки при делении на $m(x)$ совпадают. Это эквивалентно тому, что $\overline{f(x)} = \overline{g(x)}$, где $\overline{f(x)}$ – образ многочлена $f(x)$ относительно канонического гомоморфизма $\mathbb{F}_p[x] \to \mathbb{F}_p[x]/(m(x))$. Заметим, что $|\mathbb{F}_p[x]/(m(x))| = p^{\deg m(x)}$.

Определение 3.2. Для ненулевого многочлена $g(x)$ положим $|g(x)| = p^{\deg g(x)}$.

Очевидно, для любого натурального числа e и любого многочлена $g(x) \in \mathbb{F}_p[x]$ справедливо свойство

$$|g^e(x)| = p^{\deg(g^e(x))} = p^{e \deg g(x)} = |g(x)|^e.$$

Введем следующие подгруппы группы $SL_2(\mathbb{F}_p[x])$:

$$\Gamma_0(m(x)) = \left\{ \begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix} \in SL_2(\mathbb{F}_p[x]) \ : \ \begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix} \equiv \begin{pmatrix} a(x) & b(x) \\ 0 & d(x) \end{pmatrix} \ (\mathrm{mod}\ m(x)) \right\},$$

$$\Gamma_1(m(x)) = \left\{ \begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix} \in SL_2(\mathbb{F}_p[x]) \ : \ \begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix} \equiv \begin{pmatrix} 1 & b(x) \\ 0 & 1 \end{pmatrix} \ (\mathrm{mod}\ m(x)) \right\},$$

$$\Gamma(m(x)) = \left\{ \begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix} \in SL_2(\mathbb{F}_p[x]) \ : \ \begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ (\mathrm{mod}\ m(x)) \right\}.$$

Здесь и далее сравнимость матриц по модулю $m(x)$ понимают как их поэлементную сравнимость. Очевидно, что справедливы включения

$$\Gamma(m(x)) \subset \Gamma_1(m(x)) \subset \Gamma_0(m(x)) \subset SL_2(\mathbb{F}_p[x]).$$

Подгруппа $\Gamma(m(x))$ называется главной конгруэнц-подгруппой по модулю $m(x)$, остальные подгруппы – просто конгруэнц-подгруппами.

Построим сначала несколько важных гомоморфизмов.

Лемма 3.3. *Отображение* $\varphi : SL_2(\mathbb{F}_p[x]) \to SL_2(\mathbb{F}_p[x]/(m(x)))$, *где*

$$\begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix} \mapsto \begin{pmatrix} \overline{a(x)} & \overline{b(x)} \\ \overline{c(x)} & \overline{d(x)} \end{pmatrix},$$

является сюръективным гомоморфизмом с ядром $\ker\varphi = \Gamma(m(x))$.

Доказательство. Очевидно, что φ – гомоморфизм групп. Возьмем произвольный элемент $y \in SL_2(\mathbb{F}_p[x]/(m(x)))$. Пусть $M_{2\times 2}$ – множество квадратных матриц размерности 2. Тогда существует матрица

$$\gamma(x) = \begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix} \in M_{2\times 2}(\mathbb{F}_p[x]),$$

такая, что

$$y = \overline{\gamma(x)} = \begin{pmatrix} \overline{a(x)} & \overline{b(x)} \\ \overline{c(x)} & \overline{d(x)} \end{pmatrix}.$$

Заметим, что поскольку $a(x)d(x) - b(x)c(x) = 1 + m(x)k(x)$ для некоторого $k(x) \in \mathbb{F}_p[x]$, мы получаем $(c(x), d(x), m(x)) = 1$. Построим матрицу

$$\gamma'(x) = \begin{pmatrix} a'(x) & b'(x) \\ c'(x) & d'(x) \end{pmatrix} \in SL_2(\mathbb{F}_p[x]),$$

для которой $\overline{\gamma'(x)} = \overline{\gamma(x)}$, она и будет искомым прообразом.

Мы утверждаем, что существуют многочлены $c'(x), d'(x)$, для которых $c'(x) \equiv c(x) (\mathrm{mod}\ m(x))$, $d'(x) \equiv d(x) (\mathrm{mod}\ m(x))$ и $(c'(x), d'(x)) = 1$ (они дадут нам вторую строку нашей матрицы $\gamma'(x)$). Положим

$$d'(x) = \begin{cases} d(x), & \text{если } d(x) \neq 0, \\ m(x) & \text{в противном случае.} \end{cases}$$

Если $d'(x) = d' \in \mathbb{F}_p$, можно взять $c'(x) = c(x)$. В противном случае разложим $d'(x)$ на простые нормированные множители $d'(x) = \alpha P_1^{e_1}(x) \cdot \ldots \cdot P_r^{e_r}(x)$, $\alpha \in \mathbb{F}_p$. Для каждого $i \in \{1, \ldots, r\}$ определим $t_i(x) = 1$, если $P_i(x) | c(x)$, и $t_i(x) = 0$, если $P_i(x) \nmid c(x)$. Согласно лемме 3.1, существует многочлен $t(x) \in \mathbb{F}_p[x]$ такой, что $t(x) \equiv t_i(x) (\mathrm{mod}\ P_i(x))$ для всех $i \in \{1, \ldots, r\}$. Положим

$$c'(x) = c(x) + t(x)m(x)$$

и докажем от противного, что $(c'(x), d'(x)) = 1$.

Пусть это не так, тогда существует неприводимый многочлен $P(x) = P_i(x)$ такой, что $P(x) \mid d'(x)$ и $P(x) \mid c'(x)$. Если мы предположим, что $P(x) \nmid c(x)$, то по построению $t(x) \equiv 0 (\mathrm{mod}\ P(x))$ и поэтому $P(x) \mid (c'(x) - t(x)m(x)) = c(x)$?! Если же мы предположим, что $P(x) \mid c(x)$, то $t(x) \equiv \equiv 1 (\mathrm{mod}\ P(x))$ и поэтому равенство $c'(x) = c(x) + t(x)m(x)$ приводит к $0 \equiv m(x) (\mathrm{mod}\ P(x))$, откуда

следует $P(x) \mid m(x)$, $P(x) \mid c(x)$ и $P(x) \mid d(x)$, что противоречит равенству $(c(x),d(x),m(x)) = 1$. Значит, $c'(x)$ и $d'(x)$ взаимно просты.

Теперь заметим, что по построению $a(x)d'(x) - b(x)c'(x) = 1 + m(x)k'(x)$ для некоторого $k'(x) \in \mathbb{F}_p[x]$, а также существуют $f(x), g(x) \in \mathbb{F}_p[x]$ такие, что $f(x)c'(x) + g(x)d'(x) = 1$. Положив

$$a'(x) = a(x) - k'(x)g(x)m(x),\ b'(x) = b(x) + k'(x)f(x)m(x),$$

получаем $\det\gamma'(x) = 1$, а потому $\gamma'(x)$ – искомая матрица. Сюръективность доказана.

Утверждение $\ker\varphi = \Gamma(m(x))$ очевидно. □

Лемма 3.4. *Отображение* $\psi : \Gamma_0(m(x)) \to (\mathbb{F}_p[x]/(m(x)))^*$*, задаваемое формулой*

$$\begin{pmatrix} a(x) & b(x) \\ m(x)c'(x) & d(x) \end{pmatrix} \mapsto \overline{d(x)},$$

является сюръективным гомоморфизмом групп и $\ker\psi = \Gamma_1(m(x))$.

Доказательство. Это гомоморфизм групп, поскольку

$$\begin{pmatrix} a(x) & b(x) \\ m(x)c'(x) & d(x) \end{pmatrix}\begin{pmatrix} a_1(x) & b_1(x) \\ m(x)c_1'(x) & d_1(x) \end{pmatrix} \mapsto \overline{m(x)c'(x)b_1(x) + d(x)d_1(x)} = \overline{d(x)}\,\overline{d_1(x)}.$$

Докажем, что он сюръективен. Возьмем произвольный элемент $y \in (\mathbb{F}_p[x]/(m(x)))^*$. Тогда существует $d(x) \in \mathbb{F}_p[x]$: $y = \overline{d(x)}$. Так как $\overline{d(x)}$ обратим, то существует $a(x) \in \mathbb{F}_p[x]$ такой, что $\overline{a(x)}\,\overline{d(x)} = \overline{1}$. Это равносильно равенству $a(x)d(x) = 1 + m(x)k(x)$ для некоторого $k(x) \in \mathbb{F}_p[x]$. Матрица

$$\begin{pmatrix} a(x) & k(x) \\ m(x) & d(x) \end{pmatrix} \in \Gamma_0(m(x))$$

является искомым прообразом. Равенство $\ker\psi = \Gamma_1(m(x))$ очевидно. □

Лемма 3.5. *Отображение* $\xi : \Gamma_1(m(x)) \to \mathbb{F}_p[x]/(m(x))$*, из мультипликативной группы* $\Gamma_1(m(x))$ *в аддитивную группу кольца* $\mathbb{F}_p[x]/(m(x))$*, которое задается формулой*

$$\begin{pmatrix} 1 + m(x)a'(x) & b(x) \\ m(x)c'(x) & 1 + m(x)d'(x) \end{pmatrix} \mapsto \overline{b(x)},$$

является сюръективным гомоморфизмом групп с ядром $\ker\xi = \Gamma(m(x))$.

Доказательство. Очевидно, что отображение корректно определено и является гомоморфизмом. Докажем его сюръективность. Выберем произвольный элемент $y \in \mathbb{F}_p[x]/(m(x))$, для него существует $b(x) \in \mathbb{F}_p[x]$: $y = \overline{b(x)}$. Тогда матрица

$$\begin{pmatrix} 1 + m(x)b(x) & b(x) \\ m(x) & 1 \end{pmatrix} \in \Gamma_1(m(x))$$

является прообразом y. Теперь легко видеть, что $\ker\xi = \Gamma(m(x))$. □

Значок $\lhd$ как обычно обозначает нормальность подгруппы в группе.

Следствие 3.6. $\Gamma(m(x)) \lhd SL_2(\mathbb{F}_p[x])$ *и* $\Gamma_1(m(x)) \lhd \Gamma_0(m(x))$.

Доказательство. Утверждение следует из лемм 3.3 и 3.4. □

Замечание 3.7. *Однако* $\Gamma_1(m(x)) \not\lhd SL_2(\mathbb{F}_p[x])$ *и* $\Gamma_0(m(x)) \not\lhd SL_2(\mathbb{F}_p[x])$.

Действительно,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(m(x)) \subset \Gamma_0(m(x)),$$

но

$$\begin{pmatrix} 1 & 0 \\ p-1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ p-1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 1 \\ p-1 & 0 \end{pmatrix} \notin \Gamma_0(m(x)).$$

Поскольку $SL_2(\mathbb{F}_p[x]/(m(x)))$ – конечная группа, то по лемме 3.3 индекс $[SL_2(\mathbb{F}_p[x]) : \Gamma(m(x))]$ конечен. Поэтому подгруппа $\Gamma_0(m(x))$ также имеет конечный индекс в $SL_2(\mathbb{F}_p[x])$. Найдем эти индексы. Для этого введем функцию $\Phi(f(x))$ – число ненулевых многочленов степени, меньшей $\deg f(x)$, взаимно простых с $f(x)$. Справедливо

Предложение 3.8 [13, предложение 1.7]. *Пусть $P(x)$ – неприводимый многочлен, тогда*

$$\Phi(m(x)) = |m(x)| \prod_{P(x)|m(x)} \left(1 - \frac{1}{|P(x)|}\right).$$

Заметим, что $\Phi(P(x)) = |P(x)| - 1$, а $\Phi(P^e(x)) = |P^e(x)| - |P^{e-1}(x)|$.

Лемма 3.9. *Каноническое разложение многочлена $m(x)$ на простые множители:*

$$m(x) = \alpha P_1^{e_1}(x) \times \ldots \times P_r^{e_r}(x),\ \alpha \in \mathbb{F}_p,$$

индуцирует естественный изоморфизм

$$\psi : SL_2(\mathbb{F}_p[x]/(m(x))) \to SL_2(\mathbb{F}_p[x]/(P_1^{e_1}(x))) \times \ldots \times SL_2(\mathbb{F}_p[x]/(P_r^{e_r}(x))).$$

Доказательство. Инъективность отображения ψ следует из леммы 3.1. В нашей ситуации, если для матрицы $\gamma(x) \in SL_2(\mathbb{F}_p[x])$ справедливо $\gamma(x) \equiv I_2 \pmod{P_i^{e_i}(x)}$ для всех $i \in \{1,\ldots,r\}$, то $\gamma(x) \equiv I_2 \pmod{m(x)}$, где I_2 – единичная матрица размерности 2.

Теперь докажем сюръективность ψ. Пусть

$$(\overline{\gamma^{(1)}(x)}, \ldots, \overline{\gamma^{(r)}(x)}) \in SL_2(\mathbb{F}_p[x]/(P_1^{e_1}(x))) \times \ldots \times SL_2(\mathbb{F}_p[x]/(P_r^{e_r}(x))).$$

Снова применяя лемму 3.1, мы можем найти матрицу $\gamma(x) \in M_{2\times 2}(\mathbb{F}_p[x])$ такую, что $\gamma(x) \equiv \gamma^{(i)}(x) \pmod{P_k^{e_i}(x)}$ для всех $i \in \{1,\ldots,r\}$. Поскольку $\det\gamma(x) \equiv \det\gamma^{(k)}(x) \equiv 1 \pmod{P_k^{e_i}(x)}$ для всех k, то $\det\gamma(x) \equiv 1 \pmod{m(x)}$. Значит, искомый прообраз – это $\overline{\gamma(x)} \in SL_2(\mathbb{F}_p[x]/(m(x)))$. □

Предложение 3.10. *(i)* $[\Gamma_1(m(x)) : \Gamma(m(x))] = |m(x)|$;

(ii) $[\Gamma_0(m(x)) : \Gamma_1(m(x))] = \Phi(m(x))$;

(iii) $[SL_2(\mathbb{F}_p[x]) : \Gamma(m(x))] = |m(x)|^3 \prod_{P(x)|m(x)} \left(1 - \frac{1}{|P(x)|^2}\right)$;

(iv) $[SL_2(\mathbb{F}_p[x]) : \Gamma_0(m(x))] = |m(x)| \prod_{P(x)|m(x)} \left(1 + \frac{1}{|P(x)|}\right)$.

Доказательство. *(i)* Из леммы 3.5 вытекает, что

$$[\Gamma_1(m(x)) : \Gamma(m(x))] = |\mathbb{F}_p[x]/(m(x))| = |m(x)|.$$

(ii) По лемме 3.4,

$$[\Gamma_0(m(x)) : \Gamma_1(m(x))] = |(\mathbb{F}_p[x]/(m(x)))^*| = \Phi(m(x)).$$

(iii) Применяя лемму 3.9, получаем, что нам достаточно доказать утверждение при $m(x) = P^e(x)$. Из леммы 3.3 следует, что

$$[SL_2(\mathbb{F}_p[x]) : \Gamma(P^e(x))] = |SL_2(\mathbb{F}_p[x]/(P^e(x)))|.$$

Символом GL_2 обозначим множество обратимых квадратных матриц размерности 2. Поскольку гомоморфизм групп $\det : GL_2(\mathbb{F}_p[x]/(P^e(x))) \to (\mathbb{F}_p[x]/(P^e(x)))^*$ сюръективен и его ядро равно $SL_2(\mathbb{F}_p[x]/(P^e(x)))$, имеем

$$|SL_2(\mathbb{F}_p[x]/(P^e(x)))| = \frac{|GL_2(\mathbb{F}_p[x]/(P^e(x)))|}{\Phi(P^e(x))} = \frac{|GL_2(\mathbb{F}_p[x]/(P^e(x)))|}{|P^e(x)| - |P^{e-1}(x)|},$$

и нам осталось определить порядок группы $GL_2(\mathbb{F}_p[x]/(P^e(x)))$.

Естественный гомоморфизм групп

$$\zeta : GL_2(\mathbb{F}_p[x]/(P^e(x))) \to GL_2(\mathbb{F}_p[x]/(P(x)))$$

сюръективен. Действительно, если матрица $\gamma(x) \in M_{2\times 2}(\mathbb{F}_p[x])$ переходит в матрицу $\overline{\gamma(x)} \in GL_2(\mathbb{F}_p[x]/(P(x)))$, то из $\det\gamma(x) \not\equiv 0 \pmod{P(x)}$ следует, что $\det\gamma(x) \not\equiv 0 \pmod{P^e(x)}$, и поэтому матрица $\gamma(x) \pmod{P^e(x)} \in GL_2(\mathbb{F}_p[x]/(P^e(x)))$ и переходит при отображении ζ в $\overline{\gamma(x)}$. Получаем точную последовательность:

$$1 \to K \to GL_2(\mathbb{F}_p[x]/(P^e(x))) \to GL_2(\mathbb{F}_p[x]/(P(x))) \to 1,$$

где $K = \{I_2 + A(x) \mid A(x) \in P(x)M_{2\times 2}(\mathbb{F}_p[x]/(P^e(x)))\}$. Поэтому

$$|GL_2(\mathbb{F}_p[x]/(P^e(x)))| = |K| \cdot |GL_2(\mathbb{F}_p[x]/(P(x)))|.$$

Заметим, что $|\mathbb{F}_p[x]/(P(x))| = |P(x)|$. Кроме того, поскольку $P(x)$ неприводим, любой ненулевой многочлен $f(x) \in \mathbb{F}_p[x]$ либо делится на $P(x)$, либо взаимно прост с ним, т. е. существуют многочлены $q(x)$, $r(x) \in \mathbb{F}_p[x]$ такие, что $f(x)q(x) + P(x)r(x) = 1$, что равносильно сравнению $f(x)q(x) \equiv 1 (\bmod\ P(x))$. Отсюда следует, что вычет $\overline{f(x)}$ по модулю $P(x)$ обратим и $\mathbb{F}_p[x]/(P(x))$ является полем.

Заметим, что $GL_2(\mathbb{F}_p[x]/(P(x))) \cong GL_2(\mathbb{F}_q)$, где $q = |P(x)|$. Поэтому [14, §4, с. 19]

$$|GL_2(\mathbb{F}_p[x]/(P(x)))| = (|P(x)|^2 - 1)(|P(x)|^2 - |P(x)|) = (|P(x)| - 1)^2(|P(x)| + 1)|P(x)|.$$

С другой стороны, число многочленов, степень которых меньше $\deg P^e(x)$ и которые делятся на $P(x)$, равно $|P^e(x)| - \Phi(P^e(x)) = |P^e(x)| - (|P^e(x)| - |P^{e-1}(x)|) = |P^{e-1}(x)|$. Поэтому

$$|K| = |M_{2\times 2}(\mathbb{F}_p[x]/(P^e(x)))| = |P^{e-1}(x)|^4 = |P(x)|^{4e-4}.$$

Отсюда получаем, что

$$|GL_2(\mathbb{F}_p[x]/(P^e(x)))| = (|P(x)| - 1)^2(|P(x)| + 1)|P(x)|^{4e-3},$$

$$|SL_2(\mathbb{F}_p[x]/(P^e(x)))| = \frac{(|P(x)| - 1)^2(|P(x)| + 1)||P(x)|^{4e-3}}{(|P(x)| - 1)|P(x)|^{e-1}} = |P^e(x)|^3 \left(1 - \frac{1}{|P(x)|^2}\right).$$

(iv) Следует из пунктов (i)–(iii), поскольку

$$[SL_2(\mathbb{F}_p[x]) : \Gamma(m(x))] = |m(x)|^2 \Phi(m(x)) \prod_{P(x)|m(x)} \left(1 + \frac{1}{|P(x)|}\right).$$

□

Заметим, что несмотря на глубокое сходство между $\mathbb{Z}$ и $\mathbb{F}_p[x]$, а также между $SL_2(\mathbb{Z})$ и $SL_2(\mathbb{F}_p[x])$, между ними есть и существенное различие. Так, группа $SL_2(\mathbb{Z})$ порождается двумя элементами, например,

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ и } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

а для $SL_2(\mathbb{F}_p[x])$ это неверно. Х. Нагао показал в [15], что группа $SL_2(\mathbb{F}_p[x])$ не является конечнопорожденной.

Также при $e > 1$ существенно отличается строение групп $(\mathbb{Z}/p^e\mathbb{Z})^*$ и $(\mathbb{F}_p[x]/(P^e(x)))^*$ (см. [13, предложение 1.6]). Если p нечетно, что группа $(\mathbb{Z}/p^e\mathbb{Z})^*$ циклическая. Если $p = 2$ и $e \geqslant 3$, то $(\mathbb{Z}/2^e\mathbb{Z})^*$ – это прямое произведение циклической группы порядка 2 и циклической группы порядка 2^{e-2}. В то же время справедливо

Предложение 3.11. *Пусть $P(x)$ – неприводимый многочлен, а e – целое число. Пусть $(\mathbb{F}_p[x]/(P^e(x)))^{(1)}$ – ядро естественного гомоморфизма из $(\mathbb{F}_p[x]/(P^e(x)))^*$ в $(\mathbb{F}_p[x]/(P(x)))^*$. Тогда это p-группа порядка $|P(x)|^{e-1}$. Если e стремится к бесконечности, то минимальное число образующих $(\mathbb{F}_p[x]/(P^e(x)))^{(1)}$ тоже стремится к бесконечности.*

Для реализации пороговой модулярной схемы в группе $SL_2(\mathbb{F}_p[x])$ нужно получить явное описание фундаментальной области относительно подгруппы $\Gamma(m(x))$ при ее действии правыми сдвигами, что является аналогом полной системы вычетов $\{0, 1, \ldots, n-1\}$ по некоторому модулю n в кольце $\mathbb{Z}$. Ввиду леммы 3.3 это можно было бы сделать с помощью техники подъема (лифтинга), однако эта задача пока решена не в полной мере. В [16, с. 438–439] указывается, что установить возможность подъема решений целочисленного уравнения $xy - zt = 1$ по некоторой системе модулей до целочисленного решения не так-то легко. Еще больше сложностей возникает при решении такого уравнения в кольце $\mathbb{F}_p[x]$.

Нам удалось построить значительную часть этой области, что достаточно для наших целей. Дадим явное описание части фундаментальной области группы $SL_2(\mathbb{F}_p[x])$ при действии на ней правыми сдвигами группой $\Gamma(m(x))$. Укажем семейство попарно несравнимых элементов группы $\Gamma_0(m(x))$ по модулю $m(x)$ в количестве, равном $[\Gamma_0(m(x)) : \Gamma_1(m(x))] = \Phi(m(x))$. Возьмем произвольный элемент

$\varepsilon_i(x) \in \mathbb{F}_p[x]$ такой, что $\overline{\varepsilon_i(x)} \in (\mathbb{F}_p[x]/(m(x)))^*$. Тогда существует $\varepsilon_i'(x) \in \mathbb{F}_p[x]$:

$$\varepsilon_i(x)\varepsilon_i'(x) = 1 + m(x)k_i(x)$$

и $\varepsilon_i'(x)$, $k_i(x)$ однозначно определяются выбором $\varepsilon_i(x)$. Имеем

$$A_i(x) = \begin{pmatrix} \varepsilon_i(x) & k_i(x) \\ m(x) & \varepsilon_i'(x) \end{pmatrix} \in \Gamma_0(m(x)).$$

Таких матриц имеется ровно $\Phi(m(x))$, а значит, можно считать, что $i = 1, \ldots, \Phi(m(x))$. Образуем из матриц $A_i(x)$ новые матрицы:

$$B_{i,j(x)}(x) = \begin{pmatrix} \varepsilon_i(x) + j(x)m(x) & k_i(x) + j(x)\varepsilon_i'(x) \\ m(x) & \varepsilon_i'(x) \end{pmatrix} \in \Gamma_0(m(x)),$$

где $i = 1, \ldots, \Phi(m(x))$, $\deg j(x) < \deg m(x)$. Матрицы $B_{i,j(x)}(x)$ попарно различны при различных i, $j(x)$. Действительно, если $i_1 \neq i_2$, то

$$\varepsilon_{i_1}(x) + j_1(x)m(x) \equiv \varepsilon_{i_2}(x) + j_2(x)m(x) \ (\mathrm{mod}\ m(x)) \Leftrightarrow \varepsilon_{i_1}(x) \equiv \varepsilon_{i_2}(x) \ (\mathrm{mod}\ m(x))?!$$

Если $i_1 = i_2 = i$, но $j_1(x) \neq j_2(x)$, то

$$k_i(x) + j_1(x)\varepsilon_i'(x) \equiv k_i(x) + j_2(x)\varepsilon_i'(x) \ (\mathrm{mod}\ m(x)) \Leftrightarrow j_1(x)\varepsilon_i'(x) \equiv j_2(x)\varepsilon_i'(x) \ (\mathrm{mod}\ m(x)) \Leftrightarrow$$

$$\Leftrightarrow j_1(x) \equiv j_2(x) \ (\mathrm{mod}\ m(x))?!$$

Тем самым доказана

Теорема 3.12. *Матрицы $A_i(x)$ при $i = 1, \ldots, \Phi(m(x))$, составляют фундаментальную область группы $\Gamma_0(m(x))$ относительно подгруппы $\Gamma_1(m(x))$, а матрицы $B_{i,j(x)}(x)$ при $i = 1, \ldots$ $\ldots, \Phi(m(x))$, $\deg j(x) < \deg m(x)$, – фундаментальную область группы $\Gamma_0(m(x))$ относительно подгруппы $\Gamma(m(x))$.*

Таким образом мы построили часть фундаментальной области, необходимую для реализации схемы разделения секрета.

4. Пороговое модулярное разделение секрета в группе $SL_2(\mathbb{F}_p[x])$

Построим в группе $SL_2(\mathbb{F}_p[x])$ модулярное пороговое разделение секрета. Напомним, что необходимо подобрать семейство $m_1(x), m_2(x), \ldots, m_k(x) \in \mathbb{F}_p[x]$ попарно взаимно простых модулей участников. Условия $m_1 < m_2 < \ldots < m_k$ и

$$M_1 = m_{k-t+2}m_{k-t+3}\ldots m_k < m_1 m_2 \ldots m_t = M_2$$

из схемы Миньотта трансформируются в неравенство для сумм степеней:

$$M_1 = \max_{A \in \overline{\Gamma}} \sum_{j \in A} \deg m_j(x) < \min_{A \in \Gamma} \sum_{i \in A} \deg m_i(x) = M_2. \tag{4.1}$$

Очевидно, что если модули участников имеют одинаковую степень n, то неравенство (4.1) для (t,k)-пороговой схемы выполняется автоматически, поскольку оно равносильно неравенству $(t-1)n < tn$.

Тогда если многочлен $s(x)$ выбран так, что $M_1 < \deg s(x) < M_2$, то он однозначно определяется своими вычетами по любым t или более модулям $m_i(x)$ с помощью китайской теоремы об остатках (лемма 3.1). Если же вычетов меньше, чем t, то решение соответствующей системы сравнений будет отличаться от искомого $s(x)$.

Предложим следующую схему разделения секрета в группе $SL_2(\mathbb{F}_p[x])$.

1) Выбор открытых ключей (модулей) участников схемы.

В качестве открытых ключей берутся главные конгруэнц-подгруппы $\Gamma(m_1(x)), \ldots, \Gamma(m_k(x))$, где модули $m_1(x), \ldots, m_k(x)$ попарно взаимно просты и имеют степень n.

2) Выбор секрета S и частичных секретов участников.

Секретом S является матрица из фундаментальной области

$$S = \begin{pmatrix} s_i(x) + j(x)m(x) & k_i(x) + j(x)s_i'(x) \\ m(x) & s_i'(x) \end{pmatrix},$$

где $m(x) = m_1(x)\dots m_k(x)$, $(s_i(x), m(x)) = 1$, $i = 1,\dots,\Phi(m(x))$, причем $M_1 < \deg s_i(x) < M_2$,

$$s_i(x)s_i'(x) = 1 + m(x)k(x), \tag{4.2}$$

$\deg j(x) < M_2$.

Частичными секретами участников являются поэлементные вычеты этой матрицы по модулям $m_1(x),\dots,m_k(x)$. Например, частичным секретом первого участника будет образ матрицы S при каноническом эпиморфизме

$$SL_2(\mathbb{F}_p[x]) \to SL_2(\mathbb{F}_p[x])/\Gamma(m_1(x)) \cong SL_2(\mathbb{F}_p[x]/(m_1(x))),$$

что является аналогом обычного частичного секрета в схеме Миньотта.

3) Восстановление секрета S по частичным секретам подмножества участников A, где $|A| \geqslant t$.

- $m(x)$ находится автоматически.
- Нам известны $s_i(x) + j(x)m(x) \equiv s_i(x) \pmod{m_r(x)}$, $r \in A$, по китайской теореме об остатках (лемма 3.1) находим $s_i(x) \pmod{\prod\limits_{r\in A} m_r(x)}$. Найденное решение в силу выбора $s_i(x)$ будет одним и тем же по модулям $\prod\limits_{l\in A} m_l(x)$ и $m(x)$, так как $\deg s_i(x) < \sum\limits_{l\in A} \deg m_l(x)$.
- Решив сравнение $s_i(x)s_i'(x) \equiv 1 \pmod{m(x)}$, находим $s_i'(x)$. Напомним, что все модули $m_1(x),\dots$ $\dots,m_k(x)$ известны участникам.
- Учитывая равенство (4.2), многочлен $k_i(x)$ однозначно восстанавливается по формуле $k_i(x) = \frac{s_i(x)s_i'(x)-1}{m(x)}$.
- Нам известны $k_i(x) + j(x)s_i'(x) \pmod{m_r(x)}$, $r \in A$, Используя лемму 3.1, находим $k_i(x) + j(x)s_i'(x) \pmod{\prod\limits_{r\in A} m_r(x)}$. Поскольку $(s_i'(x), m(x)) = 1$, то значение $j(x) \pmod{\prod\limits_{l\in A} m_l(x)}$ восстанавливается однозначно. Так как $\deg j(x) < M_2$, отсюда получаем $j(x)$.

Таким образом, матрица S корректно восстановлена.

Работа выполнена при поддержке Государственной программы научных исследований «Конвергенция-2025», задание 1.1.01.

Литература

1. *Cramer R., Damgard I., Nielsen J.* Multiparty computation from threshold homomorphic encryption // LNCS. 2001. Vol. 2045. P. 280–300. https://doi.org/10.1007/3-540-44987-6_18

2. *Bethencourt J., Sahai A., Waters B.* Ciphertext-policy attribute-based encryption // 2007 IEEE Symposium on Security and Privacy (SP'07), IEEE, 2007. P. 321–334. https://doi.org/10.1109/SP.2007.11

3. *Benaloh J.* Secret sharing homomorphisms: keeping shares of a secret sharing // LNCS. 1987. Vol. 263. P. 251–260. https://doi.org/10.1007/3-540-47721-7_19

4. *Shamir A.* How to share a secret // Communications of the ACM. 1979. Vol. 22. P. 612–613. https://doi.org/10.1145/359168.359176

5. *Asmuth C., Bloom J.* A modular approach to key safeguarding // IEEE Transactions on Information Theory. 1983. Vol. 29. P. 156–169. https://doi.org/10.1109/TIT.1983.1056651

6. *Mignotte M.* How to share a secret // LNCS. 1983. Vol. 149. P. 371–375. https://doi.org/10.1007/3-540-39466-4_27

7. *Galibus T., Matveev G., Shenets N.* Some structural and security properties of the modular secret sharing // Proceedings of SYNASC'08, IEEE, Los Alamitos, 2009. P. 197–200. https://doi.org/10.1109/SYNASC.2008.14

8. *Galibus T., Matveev G.* Generalized Mignotte's sequences over polynomial rings // Electronic Notes in Theoretical Computer Science. 2007. Vol. 186. P. 43–48. https://doi.org/10.1016/j.entcs.2006.12.044

9. *Galibus T., Matveev G.* Finite fields, Gröbner bases and modular secret sharing // Journal of Discrete Mathematical Sciences and Cryptography. 2012. Vol. 15. P. 339–348. https://doi.org/10.1080/09720529.2012.10698386

10. *Васьковский М. М., Матвеев Г. В.* Верификация модулярного разделения секрета // Журн. Белорус. гос. ун-та. Математика. Информатика. 2017. № 2. С. 17–22.

11. *Матвеев Г. В., Матулис В. В.* Совершенная верификация модулярной схемы // Журн. Белорус. гос. ун-та. Математика. Информатика. 2018. № 2. С. 4–9.

12. *Янчевский В. И., Говорушко И. О., Матвеев Г. В.* Разделение секрета в специальной линейной группе // Информатика. 2024. Т. 21, № 3. С. 39–47. https://doi.org/10.37661/1816-0301-2024-21-3-39-47

13. *Rosen M.* Number theory in function fields. New York: Springer-Verlag, 2002. 358 p.

14. *Taylor D. E.* The geometry of the classical groups. Berlin: Herdelmann Verlag, 1992. 229 p.

15. *Nagao H.* On $GL(2;K[X])$ // Journal of the Institute of Polytechnics, Osaka City University. Series A: Mathematics. 1959. Vol. 10. P. 117–121.

16. *Платонов В. П., Рапинчук А. С.* Алгебраические группы и теория чисел. М.: Наука, 1991. 656 с.

References

1. Cramer R., Damgard I., Nielsen J. Multiparty computation from threshold homomorphic encryption. *LNCS*, 2001, vol. 2045, pp. 280–300. https://doi.org/10.1007/3-540-44987-6_18

2. Bethencourt J., Sahai A., Waters B. Ciphertext-policy attribute-based encryption. *2007 IEEE Symposium on Security and Privacy (SP'07)*, IEEE, 2007, pp. 321–334. https://doi.org/10.1109/SP.2007.11

3. Benaloh J. Secret sharing homomorphisms: keeping shares of a secret sharing. *LNCS*, 1987, vol. 263, pp. 251–260. https://doi.org/10.1007/3-540-47721-7_19

4. Shamir A. How to share a secret. *Communications of the ACM*, 1979, vol. 22, pp. 612–613. https://doi.org/10.1145/359168.359176

5. Asmuth C., Bloom J. A modular approach to key safeguarding. *IEEE Transactions on Information Theory*, 1983, vol. 29, pp. 156–169. https://doi.org/10.1109/TIT.1983.1056651

6. Mignotte M. How to share a secret. *LNCS*, 1983, vol. 149, pp. 371–375. https://doi.org/10.1007/3-540-39466-4_27

7. Galibus T., Matveev G., Shenets N. Some structural and security properties of the modular secret sharing. *Proceedings of SYNASC'08*, IEEE, Los Alamitos, 2009, pp. 197–200. https://doi.org/10.1109/SYNASC.2008.14

8. Galibus T., Matveev G. Generalized Mignotte's sequences over polynomial rings. *Electronic Notes in Theoretical Computer Science*, 2007, vol. 186, pp. 43–48. https://doi.org/10.1016/j.entcs.2006.12.044

9. Galibus T., Matveev G. Finite fields, Gröbner bases and modular secret sharing. *Journal of Discrete Mathematical Sciences and Cryptography*, 2012, vol. 15, pp. 339–348. https://doi.org/10.1080/09720529.2012.10698386

10. Vaskouski M. M., Matveev G. V. Verification of modular secret sharing. *Journal of the Belarusian State University. Mathematics and Informatics*, 2017, no. 2, pp. 17–22 (in Russian).

11. Matveev G. V., Matulis V. V. Perfect verification of modular scheme. *Journal of the Belarusian State University. Mathematics and Informatics*, 2018, no. 2, pp. 4–9 (in Russian).

12. Yanchevskiĭ V. I., Havarushka I. A., Matveev G. V. Secret sharing in a special linear group. *Informatics*, 2024, vol. 21, no. 3, pp. 23–31 (in Russian). https://doi.org/10.37661/1816-0301-2024-21-3-23-31

13. Rosen M. *Number theory in function fields*. New York, Springer-Verlag, 2002, 358 p.

14. Taylor D. E. *The geometry of the classical groups*. Berlin, Herdelmann Verlag, 1992, 229 p.

15. Nagao H. On $GL(2;K[X])$. *Journal of the Institute of Polytechnics, Osaka City University. Series A: Mathematics*, 1959, vol. 10, pp. 117–121.

16. Platonov V. P., Rapinchuk A. S. *Algebraic groups and number theory*. Moscow, Nauka, 1991, 656 p. (in Russian).