ЗАЩИТА ИНФОРМАЦИИ И НАДЕЖНОСТЬ СИСТЕМ
INFORMATION PROTECTION AND SYSTEM RELIABILITY

УДК 519.719.2
https://doi.org/10.37661/1816-0301-2024-21-3-39-47

Оригинальная статья
Original Article

Разделение секрета в специальной линейной группе

В. И. Янчевский[1], И. О. Говорушко[1]✉, Г. В. Матвеев[2]

[1]*Институт математики*
Национальной академии наук Беларуси,
ул. Сурганова, 11, Минск, 220012, Беларусь
✉*E-mail: govorushko88@gmail.com*

[2]*Белорусский государственный университет,*
пр. Независимости, 4, Минск, 220030, Беларусь

Аннотация
Цели. Решается задача по разработке математических основ модулярного разделения секрета в специальной линейной группе над кольцом целых чисел.
Актуальность задачи определяется тем, что к схемам разделения секрета предъявляется большое число требований. К ним относятся идеальность схемы, возможность проведения верификации, изменения порога без участия дилера, реализации непороговой структуры доступа и некоторые другие.
Каждая разработанная к настоящему времени схема разделения секрета не в полной мере удовлетворяет всем этим требованиям. Она обладает лишь определенной конфигурацией требуемых свойств. Разработка же схемы на новой математической основе призвана расширить список таких конфигураций, что создает для пользователя больше возможностей в выборе оптимального варианта.
Методы. Используется теория групп, модулярная арифметика и теория схем разделения секрета.
Результаты. Строится фундаментальная область относительно действия главной конгруэнц-подгруппы правыми сдвигами в специальной линейной группе матриц второго порядка над кольцом целых чисел. На этой основе предложены способы модулярного разделения секрета и его порогового восстановления.
Заключение. Дано строгое математическое обоснование корректности алгоритмов генерации частичных секретов и восстановления основного секрета в специальной линейной группе над кольцом целых чисел. Эти результаты будут использованы для изучения конфигурации свойств разделения секрета в данной группе.

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

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

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Поступила в редакцию | Received 18.06.2024
Подписана в печать | Accepted 10.07.2024
Опубликована | Published 30.09.2024

Secret sharing in a special linear group

Vyacheslav I. Yanchevskiĭ[1], Ihar A. Havarushka[1]✉, Gennadii V. Matveev[2]

[1]Institute of Mathematics
of the National Academy of Sciences of Belarus,
st. Surganova, 11, Minsk, 220012, Belarus
✉*E-mail: govorushko88@gmail.com*

[2]Belarusian State University,
av. Nezavisimosti, 4, Minsk, 220030, Belarus

Abstract

Objectives. The problem of developing the mathematical foundations of modular secret sharing in a special linear group over the ring of integers is being solved.

The relevance of the problem is reduced to the fact that a large number of requirements are imposed on secret sharing schemes. These include the ideality of the scheme, the possibility of verification, changing the threshold without the participation of the dealer, the implementation of a non-threshold access structure and some others. Every secret sharing scheme developed to date does not fully satisfy all these requirements. It only has a certain configuration of these properties. The development of a scheme on a new mathematical basis is intended to expand the list of these configurations, which creates more opportunities for the user in choosing the optimal option.

Methods. Group theory, modular arithmetic and theory of secret sharing schemes are used.

Results. A fundamental domain with respect to the action of the main congruence subgroup by right shifts in the special linear group of second-order matrices over the ring of integers is constructed. On this basis, methods for modular secret sharing and its threshold restoration are proposed.

Conclusion. A rigorous mathematical justification is given for the correctness of the algorithms for generating partial secrets and restoring the main secret in the special linear group over the ring of integers. These results will be used to study the configuration of secret sharing properties in this group.

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

For citation. Yanchevskiĭ V. I., Havarushka I. A., Matveev G. V. *Secret sharing in a special linear group*. Informatika [*Informatics*], 2024, vol. 21, no. 3, pp. 39−47 (In Russ.).
https://doi.org/10.37661/1816-0301-2024-21-3-39-47

Conflict of interest. The authors declare of no conflict of interest.

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 рас-

пределенных конфиденциальных вычислениях [3]. Такие схемы строятся на основе протоколов с нулевым разглашением.

С помощью схемы разделения секрета решается следующая задача. Пусть имеется некоторая важная информация (секрет) s и множество $I=\{1,2,\ldots,k\}$ 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.

Настоящее исследование посвящено модулярному подходу в теории разделения секрета. Основы этого подхода и теории в целом были заложены в статье А. Шамира [4], а собственно модулярный подход получил развитие в работах К. Асмута и Дж. Блюма [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 полиномов над полями Галуа. В статье [7] доказано, что модулярный подход в кольце полиномов от одной переменной над полем Галуа позволяет реализовать любую структуру доступа совершенно и идеально. Более того, модулярная пороговая схема в кольце полиномов 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.

На сегодняшний день для схем разделения секрета разработано много критериев качества, например таких, как совершенность, идеальность, верифицируемость, пригодность для реализации предпороговых структур доступа и ряд других. Схем разделения секрета, удовлетворяющих всем известным критерием качества, все еще нет. Вот почему построение новых схем, основанных на принципиально иной алгебраической базе, представляет определенный интерес. В настоящей работе в качестве такой базы предлагается специальная линейная группа и модулярное разделение секрета в ней.

1. Модулярное разделение секрета. Дадим необходимые далее определения.

Под структурой доступа Г понимают монотонное семейство подмножеств, т. е. предполагается, что для его элементов выполняется условие

$$A\in\Gamma, A\subset B\subset I\Rightarrow B\in\Gamma. \quad (1)$$

Такие подмножества называют разрешенными, а остальные – запрещенными. Структура доступа, когда разрешенными считаются подмножества A с условием $|A|\geq t$, называется пороговой, а число t, $1\leq t\leq k$, 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, и 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.

Среди СРС важное место занимают пороговые схемы. Одной из первых пороговых схем была схема Шамира. Она строится следующим образом. Рассмотрим многочлен $f(x)$ степени $k-1$ над конечным полем F_p при достаточно большом p. Объявим секретом некоторый коэф-

фициент этого многочлена, например $c = f(0)$. Распределим среди t участников информацию $f(x_i) = c_i$, $i = 1, 2, ..., t$, чтобы каждый участник знал значение c_i этого многочлена в некоторой точке x_i. Тогда по известному свойству многочленов исходный многочлен может быть однозначно восстановлен по любым своим t-парам (x_i, c_i). Это можно сделать при помощи интерполяционной формулы Лагранжа.

Модулярное разделение секрета в некотором смысле обобщает схему Шамира. Оно основано на следующем простом наблюдении (К. Асмут и Д. Блюм [5], М. Миньотт [6]). Пусть $m_1 < m_2 < ... < m_l$ – система попарно взаимно простых натуральных модулей. Если секретом является некоторое натуральное число c, а секретом i-го участника, $i \in P = \{1, 2, ..., l\}$, – наименьший неотрицательный вычет c по модулю m_i, т. е. $c_i \equiv c \,(mod\, m_i)$, то группа участников $A \subseteq P$ восстанавливает исходный секрет c путем решения системы сравнений $x \equiv c_i \,(\mathrm{mod}\, m_i)$, $i \in A$. Это можно сделать, например, с помощью китайской теоремы об остатках. Правильно найдет секрет c лишь та группа участников A, для которой выполнено условие $c < \prod_{i \in A} m_i$. Тот же принцип используется при построении схемы разделения секрета над кольцом полиномов от одной и нескольких переменных [7–9].

Замечание 1. Схема Миньотта описана выше. В схеме Асмута – Блюма пользователи находят вспомогательный секрет, как показано выше. Хранимым секретом является вычет вспомогательного по некоторому несекретному модулю.

Замечание 2. Схему Шамира можно отнести к классу модулярных схем, поскольку значение многочлена в заданной точке $f(x_0) = c$ равно остатку от деления многочлена $f(x)$ на линейный многочлен $x - x_0$.

2. Фундаментальная область в специальной линейной группе. Как уже отмечалось, целью исследования является построение модулярной схемы разделения секрета в специальной линейной группе $SL_2(\mathbb{Z})$ (напомним, что это мультипликативная группа целочисленных 2×2-матриц с определителем, равным 1). Эта группа тесно связана с исследованиями по модулярным функциям. В данной группе следует найти все необходимое для построения модулярных схем подобно тому, как это происходит в кольце целых чисел $\mathbb{Z}$. Необходимо иметь, во-первых, аналог деления с остатком, а во-вторых, аналог алгоритма CRT (Chinese Remainder Theorem, китайской теоремы об остатках).

Начнем с первой задачи. В качестве аналога кольца $\mathbb{Z}$ возьмем группу $SL_2(\mathbb{Z})$, а в качестве модуля m – главную конгруэнц-подгруппу по модулю m. Она определяется следующим образом:

$$\Gamma(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}); \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mathrm{mod}\, m) \right\}. \tag{2}$$

Здесь и далее сравнимость матриц по модулю понимают как их поэлементную сравнимость. Хорошо известно [12], что подгруппа $\Gamma(m)$ является нормальным делителем группы, а ее индекс находится по формуле

$$\left[SL_2(\mathbb{Z}) : \Gamma(m) \right] = m^3 \prod_{p|m} \left(1 - \frac{1}{p^2} \right), \tag{3}$$

где p – простые делители m.

Подгруппу $\Gamma(m)$ называют главной конгруэнц-подгруппой. Также потребуется промежуточная подгруппа $\Gamma_0(m)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(\mathbb{Z});\quad c\equiv 0\pmod m\right\}$. Известны следующие равенства [12]:

$$\left[\Gamma_0(m):\Gamma(m)\right]=m^2\prod_{p|m}\left(1-\frac{1}{p}\right),\quad \left[SL_2(\mathbb{Z}):\Gamma_0(m)\right]=m\prod_{p|m}\left(1+\frac{1}{p}\right), \tag{4}$$

где p – простые делители m.

Главная конгруэнц-подгруппа $\Gamma(m)$ действует правыми сдвигами на группах $\Gamma_0(m)$ и $SL_2(\mathbb{Z})$. Система представителей орбит называется фундаментальной областью. Две матрицы A и B принадлежат одной орбите, если $A\Gamma(m)=B\Gamma(m)$. Это условие будет удобно трактовать иначе.

Лемма. Условие $A\Gamma(m)=B\Gamma(m)$ эквивалентно условию $A\equiv B\pmod m$.

Доказательство. Условие $A\Gamma(m)=B\Gamma(m)$ означает $AA_1=BB_1$, где $A_1,B_1\in\Gamma(m)$. Поэтому $A_1=E+mA_2$, $B_1=E+mB_2$. В связи с этим $A+mAA_2=B+mBB_2$, откуда следует, что $A\equiv B\pmod m$.

Докажем обратное:

$$A\equiv B\pmod m\Rightarrow B^{-1}A\equiv E\pmod m\Rightarrow B^{-1}A\in\Gamma(m)\Rightarrow A\in B\Gamma(m),$$

что и требовалось доказать.

Для реализации пороговой модулярной схемы в группе $SL_2(\mathbb{Z})$ необходимо получить явное описание фундаментальной области относительно подгруппы $\Gamma(m)$, что является аналогом полной системы вычетов $0,1,2,\ldots,m-1$ по модулю m в кольце $\mathbb{Z}$. Это можно было бы сделать с помощью техники подъема (лифтинга), поскольку канонический гомоморфизм $\varphi_m: SL_2(\mathbb{Z})\to SL_2(\mathbb{Z})$ является сюръективным. Однако данная задача пока решена не в полной мере.

Замечание 3. Задача восстановления секрета в специальной линейной группе матриц второго порядка над кольцом целых чисел в несколько иных терминах комментируется в книге [13, с. 438, 439]: «Мы настоятельно рекомендуем читателю убедиться, что установить возможность подъема решений этого уравнения ($xy-zt=1$) по некоторой системе модулей до целочисленного решения не так-то легко».

Авторы не претендуют на решение данной задачи в полной общности. В настоящей работе удалось построить значительную часть фундаментальной области, лежащую в группе $\Gamma_0(m)$. Этого оказалось достаточно для поставленных целей.

Дадим явное описание фундаментальной области группы $\Gamma_0(m)$ при действии на ней правыми сдвигами группы $\Gamma(m)$. В соответствии с леммой укажем семейство попарно несравнимых элементов группы $\Gamma_0(m)$ по модулю m в количестве, равном $\left[\Gamma_0(m):\Gamma(m)\right]=$ $=m^2\prod_{p|m}\left(1-\frac{1}{p}\right)=m\varphi(m).$

Прежде всего получим

$$\varepsilon\varepsilon'\equiv 1\pmod m\Leftrightarrow\varepsilon\varepsilon'=1+km\Leftrightarrow\begin{pmatrix}\varepsilon & k\\ m & \varepsilon'\end{pmatrix}\in\Gamma_0(m). \tag{5}$$

Таких матриц существует ровно $\varphi(m)$, так как каждый элемент группы $\mathbb{Z}_m^*$ (как и всякой иной) имеет ровно один обратный. Все такие пары $(\varepsilon_1, \varepsilon_1'), (\varepsilon_2, \varepsilon_2'), \ldots, (\varepsilon_{\varphi(m)}, \varepsilon_{\varphi(m)}')$ попарно несравнимы по модулю *m*, а их элементы пробегают приведенную систему вычетов по модулю *m*. Образуем из матриц $\begin{pmatrix} \varepsilon_i & k_i \\ m & \varepsilon_i' \end{pmatrix}$ первый столбец таблицы размером $\varphi(m) \times m$:

$$\begin{array}{cccc}
\begin{pmatrix} \varepsilon_1 & k_1 \\ m & \varepsilon_1' \end{pmatrix} & \begin{pmatrix} \varepsilon_1 + m & k_1 + \varepsilon_1' \\ m & \varepsilon_1' \end{pmatrix} & \cdots & \begin{pmatrix} \varepsilon_1 + (m-1)m & k_1 + (m-1)\varepsilon_1' \\ m & \varepsilon_1' \end{pmatrix} \\
\begin{pmatrix} \varepsilon_2 & k_2 \\ m & \varepsilon_2' \end{pmatrix} & \begin{pmatrix} \varepsilon_2 + m & k_2 + \varepsilon_2' \\ m & \varepsilon_2' \end{pmatrix} & \cdots & \begin{pmatrix} \varepsilon_2 + (m-1)m & k_2 + (m-1)\varepsilon_2' \\ m & \varepsilon_2' \end{pmatrix} \\
\vdots & \vdots & \ddots & \vdots \\
\begin{pmatrix} \varepsilon_{\varphi(m)} & k_{\varphi(m)} \\ m & \varepsilon_{\varphi(m)}' \end{pmatrix} & \begin{pmatrix} \varepsilon_{\varphi(m)} + m & k_{\varphi(m)} + \varepsilon_{\varphi(m)}' \\ m & \varepsilon_{\varphi(m)}' \end{pmatrix} & \cdots & \begin{pmatrix} \varepsilon_{\varphi(m)} + (m-1)m & k_{\varphi(m)} + (m-1)\varepsilon_{\varphi(m)}' \\ m & \varepsilon_{\varphi(m)}' \end{pmatrix}.
\end{array}$$

Элемент *i*-й строки и $(j+1)$-го столбца таблицы имеет вид

$$\begin{pmatrix} \varepsilon_i + jm & k_i + j\varepsilon_i' \\ m & \varepsilon_i' \end{pmatrix}, \; i = 1, \ldots, \varphi(m), \; j = 0, \ldots, m-1. \tag{6}$$

Матрицы из разных строк таблицы несравнимы, так как у них несравнимы элементы на месте 22. Матрицы в одной строке таблицы несравнимы по другой причине. Сравниваем у них элементы на месте 12:

$$k_i + j\varepsilon_i' \equiv k_i + l\varepsilon_i' \pmod{m} \Leftrightarrow j \equiv l \pmod{m}, \tag{7}$$

что возможно лишь при $j = l$, так как $j, l = 0, \ldots, m-1$.

3. Пороговое модулярное разделение секрета в группе $SL_2(\mathbb{Z})$. Построим в группе $SL_2(\mathbb{Z})$ аналог модулярного порогового разделения секрета по Миньотту [6]. Напомним, что для этого необходимо подобрать семейство натуральных модулей (открытых ключей) $m_1 < m_2 < \ldots < m_k$ с условиями $(m_i, m_j) = 1$ при $i \neq j$ и существует такое *t* (порог), что всегда верно неравенство $M_1 = m_{k-t+2} \ldots m_k < m_1 \ldots m_t = M_2$. Тогда если натуральное *s* выбрано из промежутка $M_1 < s < M_2$, то оно вполне определяется своими вычетами по любым *t* или более модулям с помощью алгоритма CRT. Если же вычетов меньше, чем *t*, то решение соответствующей системы сравнений будет отличаться от искомого секрета *s*. Эту конструкцию называют (*t*, *k*)-пороговой схемой.

Предложим следующую схему разделения секрета в группе $SL_2(\mathbb{Z})$:

1. *Выбор открытых ключей (модулей) участников схемы.* В качестве открытых ключей берутся главные конгруэнц-подгруппы $\Gamma(m_1), \ldots, \Gamma(m_k)$, где модули $m_1, \ldots, m_k$ те же, что и в пороговой модулярной схеме Миньотта.

2. *Выбор секрета S и частичных секретов участников.* Секретом *S* является матрица из фундаментальной области в группе $\Gamma_0(m)$, где $m = m_1 \cdots m_k$. $S = \begin{pmatrix} s_i + jm & k_i + js_i' \\ m & s_i' \end{pmatrix} \in \Gamma_0(m)$, $i = 1, \ldots, \varphi(m)$, $j = 0, \ldots, M_2 - 1$, причем $M_1 < s_i' < M_2$.

Частичными секретами участников служат поэлементные вычеты этой матрицы по модулям $m_1,\ldots,m_k$. Например, частичным секретом первого участника будет образ матрицы S при каноническом эпиморфизме

$$SL_2(\mathbb{Z}) \to {SL_2(\mathbb{Z})}\Big/{\Gamma(m_1)} \cong SL_2\left(\mathbb{Z}_{m_1}\right), \tag{8}$$

что является аналогом обычного частичного секрета в схеме Миньотта.

3. *Восстановление секрета S по частичным секретам подмножества участников A, где* $|A| \geq t$. Секрет S восстанавливается по следующему алгоритму:

– m находится автоматически;

– s_i' находится по китайской теореме об остатках путем решения системы сравнений, причем найденное решение в силу выбора s_i' будет одним и тем же по модулям $\prod_{l\in A} m_l$ и m, так как $s_i' < \prod_{l\in A} m_l$;

– s_i находится путем решения сравнения $s_i s_i' \equiv 1 (\mathrm{mod}\, m)$. Напомним, что все модули $m_1,\ldots,m_k$ известны участникам;

– k_i находится по формуле $k_i = \dfrac{s_i s_i' - 1}{m}$;

– параметр j находится при условии, что известно, с чем сравнимо $k_i + js_i'$ по модулю m. Так как $(s_i', m) = 1$, то значение j единственно по модулю m.

Таким образом, матрица $S = \begin{pmatrix} s_i + jm & k_i + js_i' \\ m & s_i' \end{pmatrix}$ корректно восстановлена.

Пример (2,3)-пороговой СРС в группе $SL_2(\mathbb{Z})$**.** В качестве числовых модулей возьмем $m_1 = 5, m_2 = 6, m_3 = 7$. Тогда имеем схему Миньотта с параметрами $M_1 = 7 < 5\cdot 6 = 30 = M_2$, т. е. хранимый секрет следует брать из промежутка $7 < s_i' < 30$. Возьмем, например, $s_i' = 11$.

В соответствии с п. 1 предложенной схемы в группе $SL_2(\mathbb{Z})$ открытыми ключами участников будут конгруэнц-подгруппы $\Gamma(5), \Gamma(6), \Gamma(7)$. В соответствии с п. 2 секретом в группе $SL_2(\mathbb{Z})$ будет матрица из фундаментальной области в группе $\Gamma_0(m)$, где $m = 5\cdot 6\cdot 7 = 210$. Поскольку $11\cdot 191 = 1 + 210\cdot 10$, откуда $s_i = 191$ и $k_i = 10$, в качестве такой матрицы берем $S = \begin{pmatrix} 401 & 21 \\ 210 & 11 \end{pmatrix}$. Частичными секретами участников будут матрицы $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 3 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$. С помощью алгоритма CRT любые два участника правильно восстановят секрет S.

Заключение. В работе построена фундаментальная область группы $\Gamma_0(m)$ при действии на ней группы $\Gamma(m)$. Предложен алгоритм модулярного разделения секрета, где в качестве открытых ключей участников взяты главные конгруэнц-подгруппы.

Вклад авторов. *В. И. Янчевский* сформулировал и обосновал алгебраическую часть, *И. О. Говорушко* составил алгоритм и написал текст статьи, *Г. В. Матвеев* обосновал криптографическую часть.

Список использованных источников

1. Cramer, R. Multiparty Computation from Threshold Homomorphic Encryption / R. Cramer, I. Damgard, J. Nielsen // LNCS. – 2001. – Vol. 2045. – P. 280–300.

2. Bethencourt, J. Ciphertext-policy attribute-based encryption / J. Bethencourt, A. Sahai, B. Waters // Proc. of IEEE Symp. on Security and Privacy, Berkeley, CA, USA, 20–23 May 2007. – Berkeley, 2007. – P. 321–334.

3. Benaloh, J. Secret sharing homomorphisms: keeping shares of a secret sharing / J. Benaloh // LNCS. – 1987. – Vol. 263. – P. 251–260.

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

5. Asmuth, C. A modular approach to key safeguarding / C. Asmuth, J. Bloom // 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 / M. Mignotte // LNCS. – 1983. – Vol. 149. – P. 371–375.

7. Galibus, T. Some structural and security properties of the modular secret sharing / T. Galibus, G. Matveev, N. Shenets // 2008 10th Intern. Symp. on Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania, 26–29 Sept. 2008. – Timisoara, 2008. – P. 197–200. https://doi.org/10.1109/SYNASC.2008.14

8. Galibus, T. Generalized Mignotte's Sequences Over Polynomial Rings / T. Galibus, G. Matveev // 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. Finite Fields. Gröbner Bases and Modular Secret Sharing / T. Galibus, G. Matveev // J. of Discrete Mathematical Sciences and Cryptography. – 2012. – Vol. 15. – P. 339–348. https://doi.org/10.1080/09720529.2012.10698386

10. Васьковский, М. М. Верификация модулярного разделения секрета / М. М. Васьковский, Г. В. Матвеев // Журнал Белорусского государственного университета. Математика. Информатика. – 2017. – № 2. – С. 17–22.

11. Матвеев, Г. В. Совершенная верификация модулярной схемы / Г. В. Матвеев, В. В. Матулис // Журнал Белорусского государственного университета. Математика. Информатика. – 2018. – № 2. – С. 4–9.

12. Di Matteo, G. The action of $SL_2(Z)$ on the upper-half complex plane / G. Di Matteo. – Mode of access: https://www.dimatteo.is/Mathematics/Courses/Modular-forms/02-SL2Z.pdf. – Date of access: 10.04.2024.

13. Платонов, В. П. Алгебраические группы и теория чисел / В. П. Платонов, А. С. Рапинчук. – 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.

2. Bethencourt J., Sahai A., Waters B. Ciphertext-policy attribute-based encryption. *Proceedings of IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 20–23 May 2007*. Berkeley, 2007, pp. 321–334.

3. Benaloh J. Secret sharing homomorphisms: keeping shares of a secret sharing. *LNCS*, 1987, vol. 263, pp. 251–260.

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.

7. Galibus T., Matveev G., Shenets N. Some structural and security properties of the modular secret sharing. *2008 10th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania, 26–29 September 2008.* Timisoara, 2008, 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*. Zhurnal Belorusskogo gosudarstvennogo universiteta. Matematika. Informatika [*Journal of the Belarusian State University. Mathematics and Informatics*], 2017, no. 2, pp. 17–22 (In Russ.)

11. Matveev G. V., Matulis V. V. *Perfect verification of modular scheme*. Zhurnal Belorusskogo gosudarstvennogo universiteta. Matematika. Informatika [*Journal of the Belarusian State University. Mathematics and Informatics*], 2018, no. 2, pp. 4–9 (In Russ.)

12. Di Matteo G. The action of $SL_2(Z)$ on the upper-half complex plane. Available at: https://www.dimatteo.is/Mathematics/Courses/Modular-forms/02-SL2Z.pdf (accessed 10.04.2024).

13. Platonov V. P., Rapinchuk A. S. Algebraicheskie gruppy i teoriya chisel. *Algebraic Groups and Number Theory*. Moscow, Nauka, 1991, 656 p. (In Russ.).

Информация об авторах

Янчевский Вячеслав Иванович, доктор физико-математических наук, академик Национальной академии наук Беларуси, заведующий отделом алгебры, Институт математики Национальной академии наук Беларуси.
E-mail: yanch@im.bas-net.by

Говорушко Игорь Олегович, кандидат физико-математических наук, научный сотрудник, Институт математики Национальной академии наук Беларуси.
E-mail: govorushko88@gmail.com
https://orcid.org/0009-0004-9914-1635

Матвеев Геннадий Васильевич, кандидат физико-математических наук, доцент, доцент кафедры высшей математики факультета прикладной математики и информатики, Белорусский государственный университет.
E-mail: matveev@bsu.by

Information about the authors

Vyacheslav I. Yanchevskiĭ, D. Sc. (Phys.-Math.), Acad. of the National Academy of Sciences of Belarus, Head of the Algebra Department, Institute of Mathematics of the National Academy of Sciences of Belarus.
E-mail: yanch@im.bas-net.by

Ihar A. Havarushka, Ph. D. (Phys.-Math.), Researcher, Institute of Mathematics of the National Academy of Sciences of Belarus.
E-mail: govorushko88@gmail.com
https://orcid.org/0009-0004-9914-1635

Gennadii V. Matveev, Ph. D. (Phys.-Math.), Assoc. Prof., Assoc. Prof. of the Department of Higher Mathematics of the Faculty of Applied Mathematics and Computer Sciences, Belarusian State University.
E-mail: matveev@bsu.by