***И.Д. Чхайло, М.Б. Атманских, О.В. Ниссенбаум***

*Тюменский государственный университет, г.Тюмень*

**УДК 003.26**

# АЛГЕБРАИЧЕСКАЯ МОДЕЛЬ XLPS-ШИФРОВ. ИСПОЛЬЗОВАНИЕ ТЕОРИИ ПРЕДСТАВЛЕНИЙ ДЛЯ ИССЛЕДОВАНИЯ КОММУТАТИВНОСТИ ШИФРОВ

**Аннотация.** В работе исследуется алгебраическая модель XLPS-шифров методами теории представлений групп. Построены представления для базовых операций XLPS-шифра и с их помощью доказана коммутативность преобразований замены и перестановки. Определены классы актуальных задач для изучения алгебраических свойств шифров.

**Ключевые слова.** Группы, представления групп, коммутативность, XLPS-шифры.

## Введение

XLPS-шифры получили широкое распространение на рубеже столетий по причине простой реализации, высокой скорости исполнения на современных процессорах и высокой криптостойкости. В работе [1] приводится описание SQUARE – первого из таких шифров. В более поздней работе [2] рассматривается другой XLPS-шифр – AES (Rijndael).

Алгебраическая криптография становится все более популярной, однако же в ней большее внимание уделяется использованию алгебраических структур как платформ для шифрования, чем исследованию алгебраических свойств самих шифров [3].

Целью данной работы является изучение алгебраической структуры XLPS-шифров с помощью теории групп и теории представлений.

Рассмотрение шифров в качестве объектов алгебраических групп позволяет исследовать их коммутативность.

**Описание XLPS-шифров**

XLPS-шифры представляют собой систему многораундового блочного шифрования. В качестве открытого текста и шифртекста выступает набор чисел, принадлежащих некоторой группе вычетов $\mathbb{Z}_n$. Такие наборы в данной работе будут называться векторами. Каждый раунд шифрования состоит из последовательного применения следующих шифров с секретными ключами:

X – гаммирование, то есть сумма некоторого секретного вектора (ключа) с вектором открытого текста.

L – линейное преобразование. Каждая компонента вектора шифртекста выражается через линейную комбинацию компонент вектора открытого текста, то есть строка умножается на матрицу – ключ.

P – шифр перестановки. Элементы вектора меняются местами друг с другом. Ключом является подстановка, длина которой равна длине блока.

S – шифр замены. Каждый элемент меняется на какой-то другой в соответствии с таблицей простой замены. Ключ – подстановка, мощность которой равна мощности алфавита. Например, для $\mathbb{Z}_n$ это $n$.

**Описание группы**

**Определение 1.** Пусть дано некоторое множество $G$, снабженное бинарной операцией +, то есть отображением вида: $+: G \times G \to G$.

Оно называется группой [4; 9-12], если выполнены следующие аксиомы:

1) $(a+b)+c=a+(b+c)$ для любых $a, b, c \in G$
2) В $G$ существует такой элемент $0$, что $a+0=0+a=a$ для любого $a \in G$
3) Для любого $a \in G$ существует такой элемент $-a \in G$, называемый противоположным, что $-a + a = a + (-a) = 0$

Если выполнена еще и следующая аксиома, то группа называется коммутативной или абелевой:

4) $a+b=b+a$ для любых $a, b \in G$

В определении в качестве символа операции был выбран знак сложения, хотя иногда применяют и другие символы (например, знак умножения). Если в качестве операции выбрано сложение, то группу принято называть аддитивной, если умножение, то мультипликативной.

**Алгебраическая структура XLPS-шифров**

Множество шифров одного типа, отличающихся друг от друга ключом, может оказаться алгебраической группой с бинарной операцией композиции шифров, то есть их последовательным применением. Для каждого шифра существует единственная функция расшифрования, которая будет обратным элементом к шифру в группе. Нейтральным элементом будет тождественный шифр. Рассмотрим, как эта модель выглядит в отношении XLPS-шифров.

1) В гаммировании блока длинны $k$ по модулю $n$ в качестве открытого текста, шифртекста и ключа используются элементы из прямой суммы групп вида: $\mathbb{Z}_n \oplus \mathbb{Z}_n \oplus \ldots \oplus \mathbb{Z}_n = \mathbb{Z}_n^k$. Так как элементами прямой суммы являются циклические абелевы группы, то и их прямая сумма будет абелевой группой [5; 351]. Различные шифры гаммирования можно отождествить с ключами, т.е. с элементами этой прямой суммы. Композиция двух шифров гаммирования является гаммированием с ключом, равным сумме ключей этих шифров. Таким образом, эти две группы изоморфны. В частности, группа шифров гаммирования – абелева.

**Теорема 1**. Группа шифров гаммирования с операцией композиции изоморфна группе $\mathbb{Z}_n^k$.

2) Поскольку линейные шифры являются матрицами, дающими шифртекст при перемножении с вектором открытого текста, то для выполнения операции композиции эти матрицы следует перемножить. Они

образуют подгруппу полной линейной группы порядка *n*. Единственной неочевидной аксиомой группы является то, что обратная матрица также будет целочисленной. Это гарантируется невырожденностью матриц и обратимостью шифрования. Таким образом линейные преобразования с компонентами, взятыми по некоторому общему модулю, являются группой.

**Теорема 2.** Множество матриц некоторого порядка по умножению, элементами которых являются числа, взятые по некоторому модулю, является подгруппой группы невырожденных матриц.

3) Сами по себе перестановки длины *n* являются симметрической группой [5; 147-154] и обозначаются $S_n$.

4) Шифры простой замены на алфавите мощности *n*, как и перестановки на блоке длинны *n*, представляют из себя двустрочную матрицу, в верхней строке которой указаны элементы алфавита, а в нижней – элементы алфавита, на которые они заменяются.

**Теорема 3.** Множество шифров замены на алфавите мощности *n* по операции композиции является группой, изоморфной $S_n$.

Группы шифров гаммирования, линейного преобразования, перестановки и замены будут обозначаться X, L, P и S соответственно. Совокупность X, L, P и S групп будет обозначаться как XLPS-группы.

Таким образом, L, P, S – группы, X – абелева группа.

**Представление XLPS-групп.**

Представление группы [4; 31-34] – это гомоморфизм группы на группу невырожденных операторов некоторого линейного пространства, то есть квадратных матриц. В данной работе под представлением будет пониматься только изоморфизм этих групп. Рассматриваются только представления над полем вещественных чисел.

Для группы $\mathbb{Z}_n$ представление имеет следующий вид [6]:

$$1 \rightarrow \begin{pmatrix} cos\frac{2\pi}{n} & sin\frac{2\pi}{n} \\ -sin\frac{2\pi}{n} & cos\frac{2\pi}{n} \end{pmatrix}$$

Под единицей имеется в виду порождающий элемент группы. Для того, чтобы найти другой элемент группы, нужно матрицу представления единицы возвести в соответствующую степень.

Для того, чтобы найти представление группы $\mathbb{Z}_n^k$, нужно составить квадратную матрицу порядка *2n*, которая будет матрицей, состоящей из клеток на главной диагонали - представлений соответствующих элементов из $\mathbb{Z}_n$ [4; 42-45].

Линейные шифры сами по себе являются матрицами, поэтому они не нуждаются в представлении.

Для группы $S_n$ представление также известно [4; 105-117]. Если $\pi$ из $S_n$ представить в виде $\pi: i \rightarrow \pi(i)$, тогда представлением будет перестановочная матрица, у которой в ячейках $(i, \pi(i))$ будут стоять единицы, а в других ячейках будут стоять нули.

Поскольку S-группа изоморфна некоторой P-группе, то и представление у нее будет такое же.

**Действие группы на множестве**

Шифры представляют из себя действие группы [5; 419-425] на множестве открытых текстов. Поскольку открытые тексты являются внешним для группы объектом, необходимо представить их в виде, пригодном для использования с матричными представлениями.

Открытые тексты и ключи шифра гаммирования являются элементом одной группы, а операция шифрования соответствуют операции группы, выполненной над ключом и текстом. Поэтому для открытого текста будет иметь место точно такое же представление, а операция шифрования будет соответствовать умножению матриц.

Для линейной замены не требовалось представления, значит и открытый текст не требуется приводить ни к какому другому виду. Операции шифрования будет соответствовать перемножение вектора и матрицы.

Для шифров перестановки тексты тоже не требуется преобразовывать. Для шифрования необходимо умножить матрицу перестановки на вектор открытого текста.

Для шифров замены открытый текст должен быть представлен в виде матрицы, количество столбцов которой равно мощности алфавита, а количество строк равно длине блока открытого текста. Каждая строка соответствует символу открытого текста, номер которого в открытом тексте совпадает с номером строки. В этой строке на месте, которое соответствует порядку символа в алфавите, ставится единица, на всех остальных местах ставятся нули. Для шифрования необходимо умножить эту матрицу слева на представление шифра замены.

*Пример*.

Дан трехбуквенный алфавит, состоящий из цифр 1, 2 и 3. Тогда представление простой замены

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

будет иметь вид:

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Пусть также дан открытый текст (2,2), который этой заменой нужно зашифровать. Тогда он должен быть представлен в виде:

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Шифрование будет выглядеть следующим образом:

$$\begin{pmatrix}0 & 1 & 0\\ 0 & 1 & 0\end{pmatrix}\begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{pmatrix}=\begin{pmatrix}0 & 0 & 1\\ 0 & 0 & 1\end{pmatrix}.$$

Результат соответствует тексту (3,3), что отвечает этому шифру.

Таким образом, для каждой XLPS-группы найдено представление. В шифрах гаммирования открытый текст имеет то же представление, шифрование происходит с помощью умножения матриц. В шифрах линейной замены и перестановки открытый текст не изменяется, шифрование происходит с помощью перемножения вектора и матрицы. В шифрах замены текст требуется представить в специальном виде. Шифрование происходит с помощью умножения матриц.

**Свободное произведение XLPS-групп и их коммутативность**

**Определение 2.** Некоторые шифры $f_{k_1}$ и $g_{k_2}$ коммутируют, если для любого открытого текста $o$ и любых ключей $k_1, k_2$ имеет место соотношение:

$$f_{k_1}\left(g_{k_2}(o)\right) = g_{k_2}\left(f_{k_1}(o)\right).$$

Коммутативность имеет место только при применении бинарной операции в алгебраической структуре, например, в группе.

Уместен вопрос, как коммутируют между собой шифры различных XLPS-групп. Как известно, в частности, из работы [7; 68 - 75], шифры замены и перестановки коммутируют всегда. Непосредственной проверкой можно убедиться, что никакая другая пара шифров из различных групп не коммутирует. Поэтому интерес представляет поиск общей алгебраической структуры, охватывающей все четыре класса.

Для этого разумно воспользоваться свободным произведением групп [5; 343-345], в котором последовательная запись различных шифров между собой будет означать их композицию. XLPS-группы будут порождающими подгруппами данной свободной группы. Нейтральные элементы из всех порождающих групп следует отождествить с пустым словом. Такая

структура отвечает и алгебраическим свойствам, и криптографическому смыслу.

Стоит отметить, что, если бы все шифры из групп X, L, P и S коммутировали между собой, тогда строка, являющаяся элементом свободной группы, могла бы быть отождествлена с последовательным применением четырех шифров из разных классов. Получившаяся алгебраическая структура была бы изоморфна прямой сумме XLPS-групп. Такой случай означает полную внешнюю коммутативность. Коммутативность некоторых групп между собой будет обозначаться как частичная внешняя коммутативность. Обычная коммутативность группы будет обозначаться как внутренняя коммутативность.

В некоторых вариантах внешней коммутативности любой XLPS-шифр был бы однораундовым, что не в полной мере отвечает его изначальной идее. Он был бы подвержен некоторым атакам, таким как «встреча посередине», потому как шифры можно было бы расставить в более удобном для злоумышленника порядке. К тому же, при полной внешней легко находится общее представление, а значит, при известном открытом тексте и шифртексте ключ находится решением системы неоднородных линейных уравнений.

Поэтому представляет интерес вопрос о том, сколько попарно коммутируемых шифров может быть в XLPS-шифре и других системах, использующих несколько видов шифров, чтобы они сохраняли свою эффективность, и как эти шифры могут быть связаны коммутируемостью между собой. Эта задача в большей мере комбинаторная, чем алгебраическая.

**Представление свободной группы**

Для свободной группы разумно попытаться найти представление. Оно будет отвечать всем XLPS-группам и позволит исследовать внешнюю

коммутативность. Такая задача представляется крайне затруднительной. Однако, в данной работе она решена для шифров перестановки и замены.

**Теорема 4.** Для того, чтобы шифры коммутировали, достаточно, чтобы у них существовало общее представление, в котором их матрицы коммутировали бы. При этом представление должно отвечать требованию корректного шифрования.

**Общее представление для шифров замены и перестановки**

Понятно, что в векторе открытого текста можно отдельно указывать элементы, которые в нем содержатся, и отдельно указывать места, на которых они стоят. Один и тот же вектор будет иметь несколько различных способов записи. Разложив текст на две части, на одну можно будет действовать перестановкой, а на другую - заменой.

Если вектор имеет $n$ компонент, то представим его в виде квадратной матрицы порядка $2n$. В левой верхней клетке матрицы размера $n$ мы запишем компоненты в виде, необходимом для действия матрицы замены, в правой нижней – единичную матрицу. Если число компонент вектора отличается от мощности алфавита, это не приведет ни к каким проблемам, хотя количество строк в верхней части будет отличаться.

Шифрами замены будут матрицы такого же порядка, в которых в левой верхней клетке порядка $n$ будет записано, собственно, представление замены, а в правой нижней клетке того же порядка будет записана единичная матрица. В матрице шифра перестановки в левой верхней клетке порядка $n$ будет единичная матрица, а в правой нижней будет записано представление перестановки.

Например, вектор (1, 2, 2) в трехбуквенном алфавите будет записан в виде

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Замена $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ будет записана в виде

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Перестановка $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ будет записана в виде

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Теперь, чтобы зашифровать матрицу открытого текста, нужно умножить ее на соответствующую матрицу шифра. Из вида матриц замены и перестановки следует, что они коммутируют, потому как их композиция есть произведение матриц, каждая из которых состоит из двух клеток, и в каждой паре перемножающихся клеток есть единичная матрица.

**Возможные направления исследования**

1) Поиск представления вышеописанной свободной группы, центра свободной группы, других нормальных делителей свободной группы.
2) Исследование комбинаторной задачи о внешней коммутативности.
3) Изучение собственных подпространств представлений XLPS-групп.

4) Применение алгебраического подхода к построению моделей других классов шифров.
5) Изучение других свойств шифрования, например, транзитивности групп шифрования.

**Заключение**

Представляет большой интерес дальнейшее исследование алгебраической структуры шифров. В данной работе построена алгебраическая модель XLPS-шифров, найдены групповые структуры X, L, P и S шифров, построены их представления. Для шифров перестановки и замены доказана коммутативность с использованием найденного общего представления. Рассмотрены возможные подходы к изучению коммутативности и определены классы актуальных задач, связанных с такими подходами.

## СПИСОК ЛИТЕРАТУРЫ


1. Daemen J., Knudsen L.R., Rijmen V. The block cipher Square // Fast Software Encryption ’97, LNCS 1267, Ed. E. Biham. Berlin, Heidelberg: Springer-Verlag, 1997. pp. 149–165.
2. Daemen J., Rijmen V. The Design of Rijndael: AES — The Advanced Encryption Standard. Berlin, Heidelberg: Springer-Verlag, 2002. 238 p.
3. Романьков В. А. Введение в криптографию. Курс лекций. М.: Форум, 2012. 240 с.
4. Наймарк М. А. Теория представлений групп. 2-е изд. М.: Физматлит, 2010. 576 с.
5. Винберг Э. Б. Курс алгебры. 2-е изд., испр. и доп. М.: Изд-во Факториал Пресс, 2001. 544 с.

6. Вейль Г. Классические группы, их инварианты и представления / пер. с анг. Д.А. Райкова. М.: Гос. изд-во иностранной лит-ры, 1947. 408 с.
7. Агибалов Г.П. Избранные теоремы начального курса криптографии: Учебное пособие. Томск: Изд-во НТЛ, 2005. 116 с.